



**Central Bank of India**

*Department of Information Technology*

**Request for Proposal (Bid) Document**

**For**

**RFP for Augmentation / Refresh of Patch Management Solution, Active Directory (AD)  
Management Solution and Procurement of related System Software**

**Bid Number: GEM/2025/B/6170727**

**25<sup>th</sup> April 2025**

## Contents

Section-1 .....	7
Tender Details .....	7
1 Invitation for Tender Offers .....	8
2 Eligibility Criteria .....	10
3 Bid Security (Earnest Money Deposit-EMD) .....	13
4 Performance Bank Guarantee (PBG) .....	13
5 Cost of Bidding .....	14
6 Manufacturer's Authorization Form .....	14
Section-2 .....	15
Scope of Work .....	15
7 Scope of Work .....	16
7.1 Scope Summary .....	16
7.2 Detailed Scope of Work .....	22
7.2.1 Detailed General Scope .....	22
7.2.2 OEM Scope .....	23
7.2.3 Applications at DC and DRC .....	25
7.2.4 AMC/ATS for Hardware and Software Items .....	45
7.2.5 Audit Trail Requirement .....	48
7.2.6 Bidder FM Services .....	48
7.2.7 Delivery & Installation .....	48
7.2.8 Maintenance .....	49
7.2.9 RFP In-Scope Activity Set .....	49
7.2.10 Mandatory Training/ Knowledge Transfer .....	50
7.3 Facilities Management Services .....	51
7.3.1 Facilities Management Services – Scope of Work .....	51
7.3.2 Scope of Work for Onsite Engineer / OEM Facility Management Engineer .....	52
7.3.3 OEM Facility Management Scope for NUTANIX (L3) .....	53
7.3.4 OEM Facility Management Engineer .....	54
7.3.5 Service Window for Bidder and OEM Engineer .....	54
7.4 General Responsibility of the Bidder .....	54
8 Project Timelines .....	56
9 Maintenance Support .....	57
Section-3 .....	58
Terms & Conditions .....	58
10 Liquidated Damage .....	59

11 Land Border Sharing Clause.....	59
12 Monitoring & Audit.....	60
13 Bid Submission.....	61
14 Integrity Pact.....	61
15 Technical and Commercial Offers .....	62
16 Evaluation & Acceptance .....	63
17 Evaluation Process.....	63
18 General Terms.....	65
19 Service Level Agreement.....	67
19.1 Service Levels during implementation phase.....	69
19.2 System Availability .....	69
19.3 Issue Criticality Classification .....	70
19.4 Service Level Default.....	71
19.5 Performance Measurements .....	72
19.6 Penalty Computation.....	74
19.7 Availability Service Credit Computation.....	75
19.8 Tables of Incident Matrix.....	76
20 Reporting of Material Adverse Events and Incident Management.....	76
21 Insurance.....	76
22 Order Cancellation.....	77
23 Indemnity .....	78
24 Confidentiality & Non-Disclosure.....	81
25 Force Majeure.....	81
26 Resolution of Disputes.....	82
27 Format of the Letter of undertaking of Authenticity to be submitted by the Bidder. ....	82
28 Sub-Contractor/ Independent Contractor.....	83
29 Assignment .....	83
30 Execution of Contract, SLA & NDA.....	84
31 Bidder's Liability.....	84
32 Information Ownership.....	84
33 Inspection, Audit, Review, Monitoring & Visitations.....	85
34 Monitoring .....	86
35 Visitations.....	86
36 Information Security .....	86
37 Intellectual Property Rights .....	86
38 Termination.....	88

38.1 Termination for Default .....	88
38.2 Termination for Insolvency.....	88
38.3 Termination- Key Terms & Conditions .....	88
38.4 Right to Transfer IT Outsourcing Arrangements .....	89
38.5 Exit Option & Contract Re-Negotiation.....	89
39 Privacy & Security Safeguards .....	89
40 Governing Law and Jurisdiction.....	90
41 Compliance .....	90
41.1 Adherence to Cyber Security Policy .....	91
41.2 Compliance with Laws.....	92
42 Violation of Terms.....	92
43 Corrupt & Fraudulent Practices .....	92
44 Publicity .....	93
45 Entire Agreement; Amendments.....	93
46 Survival and Severability .....	93
47 Bidding Document.....	93
47.1 Amendments to Bidding Documents .....	93
47.2 Period of Validity .....	93
47.3 Last Date and Time for Submission of Bids .....	93
47.4 Late Bids .....	94
47.5 Modifications and/or Withdrawal of Bids.....	94
47.6 Clarification of Bids.....	94
48 Signing of Contract.....	94
49 Sustainable Sourcing.....	94
50 Remote Access:.....	94
51 Business Continuity and Disaster Recovery .....	94
51.1 Business Continuity Plan (BCP) .....	94
51.2 Disaster Recovery Plan (DRP).....	95
52 Obligation to Cooperate with relevant authorities in case of Insolvency/Resolution.....	95
52.1 Insolvency .....	95
52.2 Cooperation.....	95
52.3 Continued Service During Resolution.....	95
52.4 Notification .....	95
53 Data Localization.....	95
54 Authorized Signatory.....	96
55 Escrow Arrangements.....	96

Section-4 .....	97
Annexures .....	97
Checklist for Submission .....	98
Annexure 1: Conformity Letter.....	99
Annexure 2: Commercial Bill of Material .....	100
Annexure 3: Bidder's Information .....	101
Annexure 4: Letter for Conformity of Product as per RFP.....	102
Annexure 5: GOI Guidelines with Model wise classification (Make in India) .....	103
Annexure 6: Undertaking of Authenticity for Products Supplied.....	106
Annexure 7: Undertaking for Acceptance of Terms of RFP.....	107
Annexure 8: Manufacturer's Authorization Form .....	108
Annexure 9: Integrity Pact .....	109
Annexure 10: Non-Disclosure Agreement.....	114
Annexure 11: Performance Bank Guarantee .....	118
Annexure 12: Minimum Technical Specifications .....	120
Annexure 13: Bid Security (BG Format- for Earnest Money Deposit) .....	121
Annexure 14: Bidder's Particulars.....	122
Annexure 15: Compliance Certificate with respect to RBI's "Master Direction on Outsourcing of Information Technology Services" .....	123
Annexure 16: NPA UNDERTAKING.....	124
Annexure17: Land Border Sharing Undertaking Letter.....	125
Annexure 18: Cover Letter .....	127
Annexure 19: [Escalation Matrix].....	128
Annexure 20: Query Format .....	129
Annexure 21: Eligibility Criteria Compliance .....	130
Annexure 22: Guidelines on Banning of Business Dealing.....	134
Annexure 23: [Undertaking of Information Security from Bidder] .....	142
Annexure 24: [Software Bill of Material (SBOM) Format] .....	143
Annexure 25- Template for Third Party Due Diligence Questionnaire .....	144

## List of Abbreviations

AMC	Annual Maintenance Contract
APM	Application Performance Management
ATS	Annual Technical Support
BOM	Bill of Material
CBI	Central Bank of India
DB	Database
DC	Data Centre
DRC/ DRS	Disaster Recovery Centre/ Site
EMD	Earnest Money Deposit
EMS	Enterprise Management System/Solution
EPP	End Point Protection
FY	Financial year
GSI	Global system integrator
GST	Goods & Service Tax
HLD	High Level Design Document
IT	Information Technology
ITAM	IT Asset Management
LLD	Low Level Design Document
LLP	Limited Liability Partnership
MAF	Manufacturer Authorization Form
MSME	Micro, Small & Medium Enterprise
NEFT	National Electronic Funds Transfer
NS	Near Site
OEM	Original equipment manufacturer
PBG	Performance Bank Guarantee
PO	Purchase order
PSE	Public Sector Enterprise
PSU	Public Sector Undertaking
RBI	Reserve Bank of India
RFP	Request for Proposal
RTGS	Real Time Gross Settlement
SAN	Storage Area Network
SAS	Serial attached SCSI
SDR	Single Data Repository
SI	System Integrator
SPOC	Single Point of Contact
SSD	Solid state drive

# **Section-1**

## **Tender Details**

## 1 Invitation for Tender Offers

Central Bank of India, herein after referred to as the “Bank”, is a leading Public Sector Bank established in the year 1911. The equity shares of the Bank are listed in both Bombay Stock Exchange/ National Stock Exchange. The Bank is having its Central Office at Chander Mukhi, Nariman Point, Mumbai– 400021. & it’s Customer Care Department at 2<sup>nd</sup> floor, MMO Building, Fort, Mumbai 400001. Bank has completed 114 years of its service to the Nation and its millions of satisfied customers with technology oriented bouquet of user friendly services and in the field of IT we are known for providing new innovative and customer friendly services. The Bank has pan India presence through its wide network of more than 4685 plus branches, 13 Zonal Offices, 90 Regional Offices spread across the country as on 31.03.2025. The Bank also has specialized branches for catering to the specific needs of Retail customers, Industrial units, corporate clients, Forex dealers, Exporters and Importers, Small Scale Industries and Agricultural sector.

Bank intends for select a bidder for Supply, Implementation, Configuration and Maintenance of Patch Management Solution, Active Directory (AD) Management Solution and Procurement of related System Software at DC and DRC.

Bank invites online tender offers (Technical offer and Commercial offer) from eligible, reputed Bidders for Supply, Implementation, Configuration and Maintenance of Patch Management Solution, Active Directory (AD) Management Solution and Procurement of related System Software at DC and DRC

The Contract Period shall be for 5 years from the date of installation / commissioning and acceptance of respective Hardware, Software and services. Bank has the option for extending the AMC/ATS of the in scope components for additional 2 years after expiry of the contract at the same cost of 5<sup>th</sup> year AMC/ATS of this tender.

**Bank reserves the right to issue a repeat order for any of the components or services at the same price subject to a maximum of 25% of ordered quantity within 60 months from the date of Purchase Order at the same price provided INR-US\$ exchange rate does not vary by more than 10% as compared to INR-US\$ exchange rate as on the date of purchase order and above or below that price will be adjusted by the Bank as per change in exchange rate.**

The details are given below:

Tender Reference Number	GEM/2025/B/6170727
Date of RFP Issue	25/04/2025
Bid Security (EMD)	₹1,70,00,000/- (Rupees One Crore Seventy Lakh Only) in the form of Bank Guarantee issued by a Scheduled Bank other than Central Bank of India for the entire period of Bid validity (120 days) plus 3 months or by means of Banker’s Cheque / Account Payee Demand Draft /RTGS/NEFT in the account no.- 3287810289 of Central Bank of India



	(IFSC Code – CBIN0283154) with narration Tender ref no GEM/2025/B/6170727 in favor of “Central Bank Of India” and payable at Mumbai.
e-mail IDs for sending queries and Last Date for submission of queries	<a href="mailto:smitd@centralbank.co.in">smitd@centralbank.co.in</a> <a href="mailto:smcbswindows@centralbank.co.in">smcbswindows@centralbank.co.in</a> <a href="mailto:cmitd@centralbank.co.in">cmitd@centralbank.co.in</a> , <a href="mailto:smitpurchase@centralbank.co.in">smitpurchase@centralbank.co.in</a> latest by <b>02/05/2025</b> up to 11:00 hrs.  Queries to be submitted with Proof of remittance of document/Tender cost (If required).
Date and time for Pre-Bid Meeting,	<b>02/05/2025</b> at 15:00hrs.
Last Date and Time submission of Bids Mode of bid submission & online portal's URL	<b>03/06/2025</b> up to 15:00 hrs. Mode-Online Government e Marketplace (GeM)
Time & Date of Opening of technical bids	<b>03/06/2025</b> at 15:30 hrs.
Response Types	1. Technical Bid + Bid Security 2. Commercial Bid
Address for Communication	General Manager-IT Central Bank Of India Department Of IT (DIT), Plot no-26, Sector-11, CBD Belapur, Navi Mumbai- 400614 <u>Mail address:</u>  <a href="mailto:smitd@centralbank.co.in">smitd@centralbank.co.in</a> <a href="mailto:smcbswindows@centralbank.co.in">smcbswindows@centralbank.co.in</a> <a href="mailto:cmitd@centralbank.co.in">cmitd@centralbank.co.in</a> , <a href="mailto:smitpurchase@centralbank.co.in">smitpurchase@centralbank.co.in</a>
Contact Telephone Numbers	022- 27582301/2487, 67123669,

The pre bid meeting will be held in person with the bidders. For any clarification with respect to this RFP, the bidder may send their queries/suggestions, valuable inputs by email to the Bank. It may be noted that all queries, clarifications, questions etc., relating to this RFP, technical or otherwise, must be in writing only and should be sent to designated email ID within stipulated time as mentioned in the below format :

S.No.	RFP Page No.	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks

Exemption from submission of EMD shall be given to bidders, who are Micro and Small Enterprises (MSE) / Startups. The bidder who are MSE has to submit necessary document issued by NSIC and the bidder who are Startups has to be recognize by Department of Industrial Policy & Promotion (DIPP) to avail the exemption. To qualify for EMD exemption, firms

should necessarily enclose a valid copy of registration certificate issued by NSIC/DIPP which are valid on last date of submission of the tender documents. MSE/Startups firms which are in the process of obtaining NSIC certificate/ DIPP will not be considered for EMD exemption.

Tender offers will normally be opened half an hour after the closing time. Any tender received without Document/Tender Cost (If required) , will be disqualified.

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

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

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

## 2 Eligibility Criteria

The Bidder must fulfil following eligibility criteria:

#	Eligibility of the Bidder and OEM	Documents to be submitted	Compliance (Y/N)
<b>Bidder's Financial Strength</b>			
1.	Bidder should be a Registered company under Indian Companies Act. 1956/2013 or LLP/Partnership firm and should have been in existence for a minimum period of 5 years in India, as on date of submission of RFP.	Copy of the Certificate of Incorporation issued by Registrar of Companies/Registrar of firms and full address of the registered office of the bidder	
2.	Bidder should be registered under G.S.T and/or tax registration in state where bidder has a registered office	Proof of registration with GSTIN	
3.	The bidder must have an annual turnover in India of INR 150 Crores per annum in the last three financial years (i.e. 2021-22, 2022-23, 2023-24).	Copy of audited Balance Sheet and Certificate of the Chartered Accountant for preceding three FYs.	

#	Eligibility of the Bidder and OEM	Documents to be submitted	Compliance (Y/N)
4.	The bidder should have made operating profits in at least two financial years out of last three financial years. (i.e. 2021-22, 2022-23, 2023-24).	Copy of audited Balance Sheet and Certificate of the Chartered Accountant for preceding three FYs.	
5.	The bidder should have a positive net worth in last three financial years (i.e. 2021-22, 2022-23, 2023-24).	Certificate of the Chartered Accountant for preceding three FYs.	
<b>Bidder and OEM Experience</b>			
6.	The Bidder should be a certified or an Authorized partner of the OEM of the offered solution	Copy of MAF from OEMs as per format (Annexure 8) to be submitted, and confirmation from OEMs confirming the partnership level of the Bidder	
7.	Bidder/ OEMs should have service/ support infrastructure at Mumbai/ Hyderabad and should be able to provide efficient and effective support.	Submit the undertaking self-declaration on Bidder's and OEM's letter head	
8.	<p>Bidder should have experience of having implemented or provided Support for</p> <ul style="list-style-type: none"> <li>Active Directory Management Solution</li> </ul> <p>OR</p> <ul style="list-style-type: none"> <li>Patch Management Solution,</li> </ul> <p>in at least one Scheduled Commercial Bank / BFSI /PSU in India in last 5 years having minimum 1000 Office/Branches in India.</p>	<p>Credential letter OR</p> <p>Copy of</p> <p>Purchase order/ Contract copy</p>	
9.	<p>The OEM for each Proposed Product should have been implemented in at least One Scheduled Commercial Bank/BFSI having minimum 1000 Office/Branches in India in last 5 years.</p> <ol style="list-style-type: none"> <li>Active Directory Management Solution</li> <li>Patch Management Solution,</li> <li>SFTP Solution</li> <li>Load Balancer</li> </ol>	<p>Credential letter OR</p> <p>Copy of</p> <p>Purchase order/ Contract copy</p>	
<b>Bidders Compliance</b>			

#	Eligibility of the Bidder and OEM	Documents to be submitted	Compliance (Y/N)
10.	At the time of bidding, the Bidder should not have been blacklisted/debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutions for any reason or non-implementation/ delivery of the order. Self-declaration to that effect should be submitted along with the technical bid.	Submit the undertaking self-declaration on Company's letter head	
11.	At the time of bidding, there should not have been any pending litigation or any legal dispute in the last five years, before any court of law between the Bidder or OEM and the Bank regarding supply of goods/services	Submit the undertaking self-declaration on Company's letter head	
12.	Bidder/OEM should not have - <ul style="list-style-type: none"> <li>• NPA with any Bank /financial institutions in India</li> <li>• Any case pending or otherwise, with any organization across the globe which affects the credibility of the Bidder in the opinion of Central Bank of India to service the needs of the Bank</li> </ul>	Submit self-declaration on Company's letter head.	
13.	If the bidder is from a country which shares a land border with India, the bidder should be registered with the Competent Authority	Certified copy of the registration certificate	

The bidder must submit only such document as evidence of any fact as required herein. The Bank, if required, may call for additional documents during the evaluation process and the bidder will be bound to provide the same.

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

- 1) Bidders need to ensure compliance to all the eligibility criteria points.
- 2) In-case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.
- 3) In case of business transfer where Bidder has acquired a Business from an entity ("Seller"), work experience credentials of the Seller in relation to the acquired business may be considered.
- 4) Bidder must provide credential letter or installation sign off document.
- 5) Scheduled Commercial Bank does not include Payments Bank, Cooperative Banks or RRBs.

- 6) While submitting the bid, the Bidder is required to comply with inter alia the following CVC guidelines detailed in Circular No. 03/01/12 (No.12-02-6 CTE/SPI (I) 2 / 161730 dated 13.01.2012): ‘Commission has decided that in all cases of procurement, the following guidelines may be followed:
- i. *In RFP, either the Indian agent on behalf of the Bidder/OEM or Bidder/OEM itself can bid but both cannot bid simultaneously for the same item/product in the same RFP. The reference of 'item/product' in the CVC guidelines refer to 'the final solution that bidders will deliver to the customer.*
  - ii. *If an agent submits bid on behalf of the Bidder /OEM, the same agent shall not submit a bid on behalf of another Bidder /OEM in the same RFP for the same item/product.'*

### **3 Bid Security (Earnest Money Deposit-EMD)**

An amount of ₹1,70,00,000/- (Rupees One Crore Seventy Lakh Only) in the form of Bank Guarantee issued by a scheduled Bank other than Central Bank of India for the entire period of Bid validity plus 3 months or by means of Account Payee Demand Draft/ Banker's cheque /RTGS/NEFT in the account no.-3287810289 of Central Bank of India (IFSC Code – CBIN0283154) with narration Tender ref no GEM/2025/B/6170727 in favour of “Central Bank Of India” and payable at Mumbai/Navi Mumbai.

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

- 1) If a Bidder withdraws its tender during the period of tender validity specified by the Bidder; or
- 2) If the Bidder does not accept the correction of its Tender Price; or
- 3) If the successful Bidder fails within the specified time to:
  - i. Sign the Contract; or
  - ii. Furnish the required security deposit.
- 4) The EMD / Bid Security of a Joint Venture (JV) must be in the name of the JV that submits the tender. If the JV has not been legally constituted at the time of bidding, the EMD / Bid Security shall be in the names of all future partners as named in the letter of intent.
- 5) The EMD / Bid Security will be refunded to the Successful Bidder, only after furnishing an unconditional and irrevocable Performance Bank Guarantee (PBG).
- 6) The EMD / Bid Security of unsuccessful Bidders shall be returned as promptly as possible after completion of bidding process.

### **4 Performance Bank Guarantee (PBG)**

- 1) As mentioned above, the Successful Bidder will furnish an unconditional and irrevocable Performance Bank Guarantee (PBG) from scheduled commercial Bank other than Central Bank of India, in the format given by the Bank in for Performance Bank Guarantee, for 5 % of the total project cost valid for 66 months, (5 years for total project period plus 6 months for claim period) validity of PBG starting from its date of issuance. The PBG shall be submitted within 21 days of the PO acceptance by the Bidder.
- 2) The PBG so applicable must be duly accompanied by a forwarding letter issued by the issuing Bank on the letterhead of the issuing Bank. Such forwarding letter shall

state that the PBG has been signed by the lawfully constituted authority legally competent to sign and execute such legal instruments. The executor (BG issuing Bank Authorities) is required to mention the Power of Attorney number and date of execution in his / her favour with authorization to sign the documents.

- 3) Each page of the PBG must bear the signature and seal of the PBG issuing Bank and PBG number.
- 4) In the event of the Successful Bidder being unable to service the contract for whatever reason, Bank may provide a cure period of 30 days and thereafter invoke the PBG, if the bidder is unable to service the contract for whatever reason.
- 5) In the event of delays by Successful Bidder in ATS support, service beyond the schedules given in the RFP, the Bank may provide a cure period of 30 days and thereafter invoke the PBG, if required.
- 6) Notwithstanding and without prejudice to any rights whatsoever of the Bank under the contract in the matter, the proceeds of the PBG shall be payable to Bank as compensation by the Successful Bidder for its failure to complete its obligations under the contract, indicating the contractual obligation(s) for which the Successful Bidder is in default.
- 7) The Bank shall also be entitled to make recoveries from the Successful Bidder's bills or any other amount due to him, the equivalent value of any payment made to him by the Bank due to inadvertence, error, collusion, misconstruction or misstatement.
- 8) The PBG may be discharged / returned by Bank upon being satisfied that there has been due performance of the obligations of the Successful Bidder under the contract. However, no interest shall be payable on the PBG.

## **5 Cost of Bidding**

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

## **6 Manufacturer's Authorization Form**

Bidders must submit a letter of authority from their manufacturers, as per format given in Annexure, that they have been authorized to quote OEM Product.

# **Section-2**

## **Scope of Work**

## 7 Scope of Work

### 7.1 Scope Summary

- 1) Central Bank of India intends to select a proven & experienced Bidder to Supply, Implement, Configure and Maintenance of Active Directory Management Solution, Patch Management Solution, SFTP Solution, Operating Systems, Load Balancer, Antivirus etc. at the Bank's location.
- 2) Bank envisages refresh/augmentation/new purchase of its existing and new applications as per below details-
  - i. Active Directory Management Solution,
  - ii. Patch Management Solution,
  - iii. SFTP Solution,
  - iv. Operating Systems,
  - v. Load Balancer
  - vi. Antivirus

Bidder is required to Supply, Install/Implement, Configure and Maintain the following components for the period of contract:

**Table - 1**

S.No.	Software Details	Qty	Existing / New
1	Active Directory Management Solution	2 (DC – 1, DR - 1) -50000 user licenses	Existing Quest
2	Patch Management Solution	2 (DC – 1, DR - 1) -39000 (Existing)+ 6000(New) System Licenses	Existing Quest
3	Patching of RedHat Enterprise Linux 8/9(RHEL 8/9) OS on IBM LinuxOne Z systems with s390x architecture.	800 Licenses	New
4	SFTP Solution	2 (DC + DR)	New
5	Redhat VDC License Standard	10	New
6	Load Balancer	4 (2 DC , 2 DR)	New
7	Antivirus	2500	New

- 1) Bank is having solution for AD Management and Patch Management from M/s Quest. Bidder may quote the Existing Solution with renewal of AMC / ATS or provide new Solution.
- 2) Bank expects bidder to augment, supply, install, implement and provide comprehensive onsite warranty & AMC/ATS support for the proposed Solution along with its



subcomponents, as mentioned in Annexure 2: Commercial Bill of Materials, for the period of contract. Bidder is, also, required to deliver all hardware, software and its sub-components at Bank's location in-line with delivery schedule and implementation timelines mentioned in Section 8.

- 3) In-depth scope of work is outlined in Section 7 – “Scope of Work” of this RFP document. Bank seeks comprehensive proposals from the bidders who have capabilities to meet Bank's requirements and have a serious interest in providing the required services. This RFP provides information on Bank, scope of work and instructions for the preparation and submission of the RFP response.
- 4) Term of the contract shall be for a period of 5 years from the day of installation acceptance and Commissioning of respective hardware, software and services by the Bank. Bank has the option for extending the AMC/ATS of the in scope components for additional 2 year after expiry of the contract at the same cost of 5th year AMC/ATS cost of this tender.
- 5) **Bank reserves the right to issue a repeat order for any of the components or services at the same price subject to a maximum of 25% of ordered quantity within 60months from the date of Purchase Order at the same price provided INR-US\$ exchange rate does not vary by more than 10% as compared to INR-US\$ exchange rate as on the date of purchase order and above or below that price will be adjusted by the Bank as per change in exchange rate.**
- 6) Bidder shall be responsible for following:
  - End-to-end installation and implementation of hardware, software licenses and Cabling, as mentioned in Annexure 2: Commercial Bill of Materials, at Bank's identified locations including configuration and customization requirement.
  - Integration, if any, with Bank's existing application platforms, server and storage environment, enterprise network, security solutions, ticketing tools etc.
  - Adherence to Service Level Agreements (SLA) as mentioned in this RFP document and periodic monitoring and reporting of the same to Bank.
  - Provision of comprehensive onsite warranty, AMC/ATS post warranty period is over and maintenance of the in-scope components for the tenure of the contract
- 7) Procurement of the application software and other in-scope components would be at Bank's discretion. Bank is not liable or bound to procure all the solutions mentioned. Bank may ask for staggered delivery of some of the components mentioned in the RFP. Details of the same would be shared with the Successful Bidder at a later stage. Bank may undertake phase wise procurement, supply, installation, and implementations of the solution(s) and its licenses.
- 8) Bank may procure products with required quantity (not limited to specific number) and may remove any solution at any stage, at its sole discretion, from in-scope proposed solutions that are part of this RFP.
- 9) Considering the nature of the applications, it may happen that the bidder may propose a solution suite consisting of multiple features, functionalities suiting to the RFP requirements and in compliance of RBI cyber security and Outsourcing Circulars. The bidder shall provide the solutions with all such features (over and above to technical specifications) without any extra cost to the Bank. All the available functionalities should be available to the Bank. The bidders shall include all necessary expenses in

complete cost of the respective line items of the solution in Annexure 2: Commercial Bill of Materials. All costs shall be included in the line items only.

- 10) The bidder shall provide complete services for the applications under the scope including installation, implementation, integration, management, maintenance, support, audit compliance and knowledge transfer.
- 11) The solution shall include all components and subcomponents like software licenses, accessories, and the bidder should supply other components at no extra cost to the Bank (required for commissioning of the solution as a part of RFP).
- 12) The bidder shall replace and upgrade the out-of-support, out-of-service, end-of-life (EOL), End of Support (EOS) undersized infrastructure elements as soon as the respective OEM announced the same at no additional cost to the Bank throughout the 5 years of contract period. The bidder shall carry out such Replacement & up gradation of components (Appliance & Software) before due date. Failure to replace within three months of intimation by Bank will be treated as violation of SLA, Bank will procure the new solution as same, and cost will be deducted from payables/ payments as penalty or by invoking performance guarantee.
- 13) During the period of the contract, all upgrades/updates or requirements in hardware, software, licensing, implementation of upgrades/patches/version changes etc., due to whatsoever reason including but not limited to EOL or EOS, shall be done by the bidder within stipulated time but not later than one month without any additional cost to the Bank. EOS/EOL solution will not be accepted and if any solution is declared EOS/EOL during the period of contract, the bidder shall do the necessary upgrade to the latest version at no additional cost to the Bank and with minimum downtime, at no additional cost to the Bank.
- 14) The bidder should inform to the Bank if any new version/update/service pack/upgrade of the proposed solution is released by OEM, within seven (7) days of such release and provide the upgraded solution within one month of such release without any cost to the Bank covering all parts, labour and accessories at the respective locations (DC and DR) of the Bank during the period of the contract. Bidder has to factor in UAT setup for the in scope applications in the RFP. For the UAT setup bidder has to provide extra licenses over the licenses mentioned in the Bill of Material Annexure -2.
- 15) The bidder shall follow all respective technical/statutory guidelines, validations should be implemented, checked & verified, and related reports including SOP, Software Integrity Certificate and VAPT Clearance must be submitted, duly certified by OEM to the Bank for sign off the successful installation.
- 16) Post installation of Solution with its components including OS, VA & PT (Vulnerability Assessment & Penetration Testing) shall be conducted, and Bank Information Security Team will provide a report to the Successful Bidder. All findings/issues pointed out in the report to be complied/fixed before commissioning and sign-off of the software (All components i.e. operating System, Database, application). The InfoSec Team and Other statutory authorities conduct review/ audit of the solutions time to time. All such Audit reports including VAPT Reports to be complied / attended by bidder/OEM within the timelines, during the entire period of contract also conduct periodic review audit of the database and application.

- 17) The solution deployment should be compliant with Bank's IT Security policy and Cyber policies, internal guidelines, regulatory standards and countrywide regulations and laws from time to time.
- 18) The proposed Solution should integrate with Bank's platforms like Security Operation Centre (SOC), Preventive Identity Management (PIM), Security Incident Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) to meet security and compliance requirements as and when required.
- 19) The bidder must provide detailed architecture of the proposed solution/ every module along with installation and administration guide, which must include high-level design (HLD), and Low Level Design (LLD) along with Technical bid. Architecture Diagram of proposed & implemented solution as actual in the Bank environment.
- 20) The Proposed solution should be free from any kind of vulnerabilities and as and when vulnerabilities are notified by the auditor, Bank, regulators, Govt. of India or any other Govt. agencies, it should be patched within prescribed time with no cost to Bank within the contract period.
- 21) The bidder shall do regular backup of the solutions as per the defined Bank's backup policy.
- 22) The Bidder shall be responsible for delivering the solution and its support post implementation. The proposed solutions should be integrated with Banks existing and new Security Solutions. The integration with Bank's existing security solutions will be in the scope of bidder with no extra cost to the Bank. In case, if any OEM can't integrate with a third party monitoring tool for an OEM product, then the bidder needs to bundle OEM tools in his response to the bid. (Performance, Availability, Patching, Monitoring, Dashboard with Graphical representation)
- 23) Deployment of solution requires coordination with different service provider / project application vendors. The bidder shall coordinate with all solution providers/ vendors while installing and ensure installation and commissioning for running the application.
- 24) The bidder shall confirm the integrity of the software supplied i.e. the software is free from bugs, malware, covert channels in code etc. and Integrity certificate should be submitted to the Bank as per the related format.
- 25) The Proposed Solution should support all heterogeneous OS, Database, Hypervisor Platforms etc.
- 26) The bidder has to do Escrow Agreement for the in-scope Solutions including all the parties at no extra cost to Bank. Bidder may quote the same in the Bill of Materials.
- 27) The proposed solution must have redundancy at all levels e.g. network redundancy (for management network interfaces), Application High Availability and power-supply redundancy at hardware/ software level required to achieve the high availability/ redundancy as per defined SLA/uptime.
- 28) The critical data / database should be stored in encrypted form.
- 29) Proposed solutions should have very high-scale architecture on a platform that scales efficiently. The solution should also support 64-bit architecture environments for high scalability. Solution should support installation on Windows and various flavours of the Linux environment. Solutions should have extensible architecture for easy integration and automation. Solution installation should support Virtual cloud for easy, deployment and building on premises. Should support multiple-deployment options - centralized, distributed and hybrid deployments with option for a centralized operations

console view. The architecture should support High Availability inbuilt into the product.

30) The bidder shall supply all modules, Software Applications with required licenses and do the installation, integration configuration & deployment of the solution at the Bank's DC and DR Site.

**31) The Annual Maintenance Cost should be minimum 8% per year of the cost of respective Product cost.**

**32) The Annual Technical Support should be minimum 20% per year of the cost of Product/ Service/ License**

**For example-**

- **If the solution cost for a particular item is Rs.100 as quoted for specific solution. In that case, AMC cost of Solution shall be of minimum 8 % of total cost of solution cost for that item i.e. Rs.8 per year. And AMC cost for two years should be minimum =  $8 \times 2 = 16$  % of total solution cost as quoted for respective line items.**
- **If the solution cost for a particular item is Rs.100 as quoted for specific solution. In that case, ATS cost of Solution shall be of minimum 20 % of total cost of solution cost for that item i.e. Rs.20 per year. And ATS cost for four years should be minimum =  $20 \times 4 = 80$  % of total solution cost as quoted for respective line items.**

33) The bidder has to provide Facility Management services at Central Bank of India DC & DR locations or any other location where centralized operation is proposed in future by deploying the professionals to support 24x7x365 days basis with shift duty hours for managing and maintaining the solution mentioned in this RFP.

34) The bidder would be responsible for updates, patches, bug fixes, version upgrades, and firmware upgrade.

35) Bidder is required to provide details of each individual proposed hardware, application software and other in-scope components along with its associated hardware & software and any other component/service necessary for installation and implementation, as mentioned in Annexure 2: Commercial Bill of Materials.

36) All necessary Racks, Power strips, Power cables, Network cables, Fibre cables and any other components required for successful implementation of the solution are to be supplied and commissioned by the Successful Bidder at no additional cost to the Bank.

37) Post implementation of the solutions, the scope of successful bidder contains support for the following activities, but not limited to, from time to time, in relation to maintenance and upgrades/updates/patches:

- Firmware/ IOS Upgrades / up to date patching,
- Faulty Parts replacement,
- Hardware System monitoring,
- Troubleshooting & Performance Tuning,
- Operating System Upgrades,
- Upgrades of supplied software,
- Advisories on software upgrades & vulnerabilities,
- Support during DR Drills,
- OS Administration & patching as per OEM guidelines

- VA / PT Compliance/Audit /Review as per Bank's requirement /Statuary guidelines
  - Any support required to make system & solution up and running as per SLA.
- 38) The list mentioned above is the indicative list; however, the successful bidder should provide end-to-end support and repair for any activities and resolution of any issues related to new deployment without any extra cost to the Bank.
- 39) Bidder must give the complete SOP (Standard Operating Procedure) document (Hard Copy & Soft Copy) before the sign off of the complete project as per Bank. SOP document should cover all the steps and troubleshooting required to install the products. SOP document should also include various basic steps to operate the devices, to create any policy/rules, to take backup, to restore, to configure reports etc.

**Responsibility matrix for the delivery, implementation and management of the proposed solution at DC, DRC**

S. N	Activity	Responsibility	To be performed by	Remarks
1	Delivery of hardware and associated software	Bidder	Bidder	Bidder will deliver the required hardware and associated software
2	Review of High Level and Low-Level Design for all Components	Bidder	OEM	a) Review the identification and formulation strategy to achieve Design Goals
				b) Review the schema design to achieve Design Goals
				c) A comprehensive report for all above activities should be submitted within one week of the completion of activities
3	Installation, configuration, and operationalization	Bidder	OEM	OEM will do the installation, configuration and operationalization of the supplied hardware and software
4	Post installation validation	Bidder	OEM	a) Assisting in formulating the process documentation
				b) Assist in performing checks to ensure installation success
				c) A comprehensive report for all above activities should be submitted within one week of the completion of activities
5	AMC/ ATS	Bidder	Bidder	1. The bidder needs to provide the necessary AMC and ATS for the tenure of the contract for the proposed solution.
				2. Bidder is required to factor in AMC for 5 years
6	Training	Bidder	OEM	For each module 3 days 2 batch of trainees

S. N	Activity	Responsibility	To be performed by	Remarks
7	FMS	Bidder	Bidder/OEM	FMS for the in-scope items will be provided by Bidder/OEM during the period of the contract.

## 7.2 Detailed Scope of Work

This section covers the broad set of requirements for the software licenses and Hardware components to be deployed at the Bank.

### 7.2.1 Detailed General Scope

Bidder is required to Supply, Install/Implement, configure and maintain the components of Table -1 for the period of contract:

- 1) The implementation shall be done by OEM/OEM Authorised Engineer, the bidder shall do back-to-back agreement with OEM for the same. The bidder shall provide Implementation Plan with Implementation methodology duly signed by OEM and Bidder.
- 2) Bidder is, also, required to carry out activities given in the following table:

Sr. No.	Activity	Remarks
1	Delivery of in-scope Hardware and Software; in at DC and DRC, as per Annexure 2: Commercial Bill of Materials	Bidder has to deliver Hardware and software, at DC and DRC, as per Annexure 2: Commercial Bill of Materials, at Bank's site
2	End-to-end installation and implementation of Hardware and Software at DC and DRC	OEM/OEM Authorized Engineer is required to do end-to-end installation, implementation and configuration of in-scope Hardware and Software.  Post end-to-end installation and implementation of software licenses, Bank will conduct acceptance test to verify installation/implementation of Hardware and Software.
3	Provide comprehensive onsite warranty and AMC / ATS support for the tenure of contract	Bidder will be responsible to provide comprehensive on-site warranty and back-to-back support from the OEM to meet the Service Levels defined in this RFP till currency of the Contract.  Warranty of Hardware and software will start from the date of installation and commissioning acceptance by Bank. AMC / ATS will start from the date of expiry of warranty period.
4	Migration Services	Bidder/OEM will be responsible to provide migration services as per the scope defined in this RFP.

- 3) Bank's Data Centre (DC) is located in Mumbai and Disaster Recovery Centre (DRC) is in Hyderabad. The bidder shall install the solution On-site at DC and DR and implement the same at all branches/offices of the Bank.
- 4) For in-scope Hardware, software, application software and cabling as mentioned in this RFP document and in Annexure 2: Commercial Bill of Materials, bidder should avoid quoting components going end-of-sale within 24 months of its date of delivery.
- 5) The proposed solutions shall be tightly integrated with all existing setup and new infrastructure /Assets Inventory Software of the Bank. The successful bidder shall supply, implement and maintain these IT Tools/ Solutions for Bank's IT Infrastructure for a period of 5 years.
- 6) Bidder should ensure that proposed hardware and software components should not go end of-life or end-of-support within 7 years of date of delivery of the device/s, the same responsibility shall so survive even after termination or expiry of the contract.
- 7) The delivery plan must be synchronized with the project delivery timelines of Bank. (Refer Section 8 of this document for Project Delivery timelines)
- 8) Bidder is required to provide resources, which may be required for successful completion of the entire assignment within the quoted cost to Bank.
- 9) All in-scope hardware should be provided with 3 years of comprehensive on-site warranty which will start from the date of installation acceptance of the respective hardware/software by Bank. Post warranty period completion, bidder should provide onsite AMC for the period of 2 years. For all the in-scope software, bidder should provide 1 year of warranty and 4 years of ATS. Bidder is required to co-ordinate with Bank's existing System Integrator for Facilities Management Services throughout the contract tenure.
- 10) As per the applications in the tender document bidder has to provide Facility Management Services which will be decided on the Banks Discretion.
- 11) The proposed solutions should coexist with all the other applications like DLP, Application Whitelisting solution, Anti-virus, Software distribution tool etc. functioning in the Banks environment without affecting any of the applications performance and Security.
- 12) For Bill of Material and Minimum Technical Specifications details refer to Annexure 2: Commercial Bill of Materials and Annexure 12: Minimum Technical Specifications.
- 13) Any open or community version of software / application is not allowed to be used in the Bank. The Bidder should quote only OEM supported version of the software /application.

### **7.2.2 OEM Scope**

- 1) For being committed to the success of the project and take ownership during the actual implementation, it is the responsibility of the bidder to ensure requisite support from the OEM for various aspects of project including configuration, performance tuning, implementation support, setting up of Production and UAT environment. The Bidder shall assess the requirement of services from OEM(s) for all the supplied applications & Hardware, and provision for requisite support.
- 2) Bidder must provision for qualified personnel to ensure highest standards during implementation phase.
- 3) During implementation OEM involvement should be spanning across all phases of implementation including Project Preparation, Solution Design Phase (Including Review/design of all the Documents, HLDs/LLDs/ Blueprints and other Solution documents), Installation, Migration (if applicable, Configuration and Customization, Integration, Acceptance and Training).

4) Below mentioned activities are to mandatorily be done by the product OEM –

S. N	Deliverable	Application OEM Responsibility
1	Project Plan	OEM(s) to review the Project plan submitted by the Bidder for their respective solution.
2	Training	OEM(s) have to mandatorily provide training to the Core team Technical & Administrative). It is also the responsibility of the OEM(s) to provide training manuals to each participant. All training material should be in English and should include Specific architecture and layout done for Bank. However, it is the responsibility of the Bidder to arrange and manage the training schedules. Training will be for 2-3 days for around ten resources at Bank's location where the required Infrastructure will be provided by the Bank.
3	HLD/ LLD	Bidder to take inputs from the OEM(s) and provide LLD & HLD documents to the Bank. However, it is the responsibility of the OEM(s) to review and recommend a methodology to achieve best performance. The same needs to be implemented upon sign-off on the documents by the Bank.
4	Data Migration Strategy (Application, Database, Storage, Backup and LTO)	OEM(s) to validate the Data Migration Approach prepared by the Bidder which should broadly include Transaction Data, the approach for customer data, execution of migration utilities on the data and resolving the issue for any inconsistency in the data.
5	Base Product Patches	OEM(s) to provide all patches related to Product, Customizations and Interfaces within the agreed timelines. OEM(s) to reconcile the product and other patches provided to the Bank in a manner that the same is available on Day 1 to the Bank.
6	Go-Live	Installation by OEM(s) and OEM(s) to assist in having hygiene factors in place for checks and closures of SIT/ UAT/ correctness of data. OEM(s) should be available during the Go-live period to address any bugs raised during the go-live phase.
7	Status Reports	OEM(s) till implementation closure is required to be a part of the status calls from an application point of view to provide timelines for bug closures.
8	Documentation	OEM(s) to share the following: <ul style="list-style-type: none"> <li>• Product manuals</li> <li>• Technical manuals</li> </ul>



### 7.2.3 Applications at DC and DRC

- 1) Bank proposes to provide the virtual servers in its on-premises Nutanix Private Cloud for deployment of in-scope Applications on x86 Platform on Windows / Redhat Linux Operating System. However, bidders are free to quote exclusive hardware as a part of their proposed solution, if the solution cannot be deployed on the Bank's private cloud by giving proper technical justification in the technical bid. Bidder should provide technical configuration of such hardware in technical bid and also include the cost including warranty/AMC/ATS or any other support cost in the commercial bid of this RFP. Bank will not pay any extra cost to the bidder for any kind of hardware and software required for the solution during the contract period. The bidder has to install and maintain the Operating System and Database of the Solutions.
- 2) Bidder has to provide proposed deployment architecture in the technical bid.
- 3) The solutions should have dashboard providing license deployments for all components, security settings, performance and other relevant information's pertains to proposed solutions. The dashboard should be customizable and with role-based admin facility.
- 4) The solution should have the capability to export results, reports, and extracts in all the standard formats like csv, pdf and any other feasible formats.
- 5) All the proposed solution should run on ORACLE Database. **In case the solution requires any other Database, the bidder has to quote the same in their bid and provide the licenses.** Bank has executed Unlimited License Agreement (ULA) with ORACLE and the same will be provided by Bank. The Oracle features available under ULA are as below:
  - Oracle Database Enterprise Edition
  - Oracle Real Application Clusters
  - Oracle Partitioning
  - Oracle Diagnostics Pack
  - Oracle Tuning Pack
  - Oracle Web Logic Suite
  - Oracle Advanced Security
  - Oracle Data Masking and Sub-setting Pack
  - Oracle Advanced Data Guard
- 6) The bidder should ensure that all these features available must be applied in database of the solution. In case bidder wants to install any other Database the bidder has to provide Database in their bid with Licenses, Software Assurance. The bidder has to provide and install all updates, Version upgrades till the contract period without any extra cost to Bank.
- 7) Bank will provide VM with Windows /Red Hat Linux OS and Oracle Data Base for implementation of proposed application. If anything else is required for successful operationalization of the proposed solution, the same has to be provided by the bidder without any additional cost to the Bank.
- 8) For the Solutions, Bank may at its discretion will do Site Visit and/or ask the bidder to do POC and Solution Presentation of the tender components and specifications at Banks location and Bank has a right to disqualify Proposed Solution on the basis of same. For the POC bidder may have to provide necessary Hardware and Software and its transportation at no cost to Bank.

### **7.2.3.1 Scope**

- 1) Bank is using Active Directory Services (ADS) for authentication and authorization of users which is running on Windows 2016 Server Operating System. Bidder is required to design, size, supply, implement and maintain Active directory Management solution at Banks DC and DR with DNS services for AD users. Bank intend to purchase a solution with minimal manual intervention for administration activities like password reset, new User ID creation etc. with self-service portal. The Solution should include effective management of resources, user accounts and their passwords, network shares, servers, printers, etc. Solution should be capable to generate various customizable reports for effective management.
- 2) The Solution is required to perform group policy management, ensure users can access only the resources they are privileged, in order to provide a secure infrastructure, automate, track, alert on changes, and automate AD data backup and recovery to mitigate downtime in the event of an outage.
- 3) Required Server on virtualized infrastructure and Network infrastructure, Bandwidth, Windows/Red Hat Linux Operating System, Oracle Database in DC/DR for implementation of the Active Directory Management and Patch Management Solution will be provided by the Bank. Any other software (including Database, Application), OS licenses, Load Balancer etc. for configuring the complete solution will be supplied by the bidder.
- 4) The bidder should provide the tentative specifications of the required hardware and OS needed at DC and DR while submitting the bid and also specify the Bandwidth requirement for DC-DR replication.
- 5) Bidder will provide a detailed formulated project plan with timelines for the implementation of the infrastructure.
- 6) While submitting the bids bidder has to submit HLD and LLD of AD Management Solution and Patch Management Solution. The successful bidder has to submit the HLD and LLD of AD Management Solution and Patch Management Solution after validation from the OEM.
- 7) Successful Bidder will provide knowledge transfer/ training to Bank and their FM Service Provider for the Solutions.
- 8) All the licenses should be perpetual

### **7.2.3.2 SCOPE OF WORK**

- 1) Active Directory Management Solution
- 2) Patch Management Solution

The bidder may meet the Scope of work requirement through a Product or combination of various products from different OEM's.

### **Existing Infrastructure**

1. Currently Bank is having Quest based Active Directory Management Solution with the following Licenses :

<b>SR No.</b>	<b>Product Name</b>
1	Change Auditor for Active Directory
2	Enterprise Reporter for Active Directory
3	GPO ADmin Enterprise
4	One Identity Manager
5	KACE Systems Management Appliance
6	Password Manager

## **BROAD SCOPE OF WORK**

### **1) Active Directory Management Solution**

The following should be configured in the Active directory Management Solution:

1. Active directory Management.
2. Self-service portal.
3. Audit and accounting - Change Auditor
4. Automated Provisioning and DE provisioning of users in AD with sync to People soft HRMS Solution.
5. Backup and restore
6. Windows Configuration
7. Custom Scripts Deployment
8. AD Reporting

### **2) Endpoint and Patch Management**

To deploy a comprehensive, secure, scalable, and centrally managed solution for the efficient management of Bank Systems across the Bank's geographically distributed infrastructure. The solution must enable automated patching, asset tracking, software compliance monitoring and remote operation execution while maintaining regulatory compliance and minimizing operational risks. The following should be configured in the Solution:

1. Patching and upgrade of Windows Endpoint and Server
2. Patching of Red Hat Linux Servers on all platform
3. Patching of other flavours of Linux Servers
4. Remote App/Patch deployment Solution
5. Inventory Management of IT and Non IT Assets (Hardware and Software)
6. Software Deployment
7. Software and Application Control Whitelisting and Blacklisting
8. Remote Access Support Management

## **Active Directory Management Solution**

1. The bidder is required to integrate all servers and desktops running on Windows etc. through Active Directory.

2. The Solution should be able to streamline user and group administration through provisioning & de-provisioning, solve security issues – and meet those never-ending compliance requirements by managing and securing on-premise AD simply and efficiently with a single, intuitive solution.
3. The Solution should be able to track changes in AD like User creation/deletion/modification, Groups, group policies, DNS. Provide alerting and reporting for the critical changes. Capability to provide all regulatory compliance reports.
4. The Solution should be able to provide deep visibility into Active Directory (AD) users, groups, roles, organizational units and permissions by providing detailed reports on various aspects of it. Apart from reports, it should also perform security assessments, configuration change history reviews etc.
5. The Solution should be able to provide functionality which helps in automate backups and quickly recover everything from a single object to an entire forest, in the event of a major disaster or corruption.
6. The bidder will be responsible to design Group Policy settings templates which follow OEM's best practice applicable for different Operating Systems. Bank and the SI will jointly decide the applicability of these templates in various environments in the Bank.
7. Daily report and all reports need to be configured as per Bank's requirement along with input like health status of AD, Number of User added and deleted and all other reports required by Bank. All reports should be system driven through Reporting module.
8. Daily/Monthly/Quarterly/yearly or whenever report to be configured as per Bank requirement with details like AD inactive user list, Health status etc.
9. Reviewer-Approver facility for Role based access and Real time notifications for the administrative activities.
10. Dashboard for day-to-day activities, reports and Domain health check-up.
11. Automated User provisioning and Bulk User management.
12. Automation of moving one-month (or as per the period defined by Bank) Inactive AD account to disable state.
13. The Solution should be able to track changes in AD like User creation/deletion/modification, Groups, group policies, DNS. Provide alerting and reporting for the critical changes. Capability to provide regulatory compliance reports.
14. The Solution should be able to provide deep visibility into Active Directory (AD) users, groups, roles, organizational units and permissions by providing detailed reports on various aspects of it. Apart from reports, it should also perform security assessments, configuration change history reviews etc.
15. The proposed solution should be able to monitor privileged activities across MS windows/cloud environment.
16. The solution should have ability to monitor access to critical files and data and should be able to identify changes in the file system.
17. The solution should have a capability to generate comprehensive change reports from compliance purpose.

18. Bidder should provide AD based single sign on (SSO) for on-premises and cloud application.
19. Enforces granular password policies across AD.
20. Notify user (email & SMS) on impending password and account expiration.
21. Automatically sync AD password in real time across multiple applications.
22. Installation of Multi Factor Authentication Solution for login to Active Directory by users. Bidder has to integrate and create customization in proposed system to proposed multi factor authentication (MFA) Solution. Setting up Multi factor authentication on top of SSO for ensuring better security. Same can be achieved by usage of TOTP/software, biometric token as per the best practices.
23. Setting up certificate servers for 300 applications scalable to 450.
24. Creation of certificate for internal application and its management.
25. Setting up SSO for all the home grown application, systems deploys at Bank.
26. Implementation of reporting/management tools which will make seamless AD Operations.
27. Provisioning for Back up and smooth restoration.
28. DC-DR replication and switching over.
29. Designing of wall paper and ensuring deployment in all AD enabled PC.
30. HLD (High level design) and LLD (Low level design) of AD Management Software Solution validated by OEM.
31. Whenever any new threats / vulnerabilities become public, the bidder/successful bidder shall bring this to the notice of the Bank immediately and help/guide the Bank in plugging the same. Once the call has been attended, successful bidder OEM shall put their maximum efforts and deploy their best resources to resolve all calls at the earliest possible time frame at all locations and ensure appropriate uptime.
32. Proposed system should proactive, approach to AD Management. Complete GUI feature for user management, user life cycle, privilege allocation and revoke, various report for top management such as users under OU, transfer of users from OU to other, user revoke or disable, number of users logged in in real time basis, number of users successfully logged in for last day, last 7 days, last month etc. with complete details of user such as employee id, name, designation etc. Extraction of report in pdf, excel and machine printable format.  
Cluster and replication status of the AD system, system monitoring etc.
33. Provide ease interface and method by hardening proposed Active Directory system
34. System should be tightly integrated Bank's SIEM, SOAR with attack insights for timely respond and stop attacks.
35. System should Flexible, lightweight deployment secures Active Directory wherever system should be agent less
36. Imposing of restriction on the AD enabled to prevent by pass.
37. Disabling of workgroup users/local user by adoption of third party or out of box customization
38. Review-Approve facility for all admin activities. Privileged access for Users.
39. Provide restricted privileges for a Technician to perform only specific tasks/roles.
40. Maker and Checker should be configured for all changes.

41. Solution should have the capability to create, modify, move, manage, enable/disable, delete, and restore the Single/Bulk Users without using any manual scripts.
42. Integration with other related systems: Any change made in Active Directory should be propagated to other connected applications and systems & vice versa including HRMS People soft.
43. The clean-up should be configured to run every month as and when required to remove the users based on certain conditions and consolidated task reports to be sent to relevant stakeholders upon clean up.
44. Should be configurable with roles that can be used to delegate task to help desk technician and other department members.
45. Solution should have risk based authentication to secure AD password resets.
46. Solution must have option to hide Group Policies.
47. Solution should be able to Disable the accounts automatically on expiry of validity period.
48. Solution should be able to Provision user accounts in bulk and assign them the privileges they need, all in one action.
49. Solution should be able to Facilitates notification to concerned users on completion of the execution of a task.
50. Solution should be able to automatically lockdown privileged accounts that are inactive for a period of time.
51. Solution should be able to Create privileged roles for task delegation and Audit the actions performed by these Delegates, including what action was performed on what object and when.
52. Solution should be able to Protect privileged accounts from password attacks by enabling advanced password policy requirements, including a dictionary rule.
53. Computer Management: Create, modify, move, manage, enable/disable, delete, and restore the Single/Bulk Computers without using any manual scripts.
54. Group Management: Create, modify, move and delete the Single/Bulk Groups without using any manual scripts.
55. OU Management: Create, modify, move and delete the Single/Bulk OUs without using any manual scripts.
56. Administrator Management: Review-Approve facility for all admin activities. Privileged access for Users.
57. GPO Management: Create, modify, and manage the GPOs. Link the GPOs to users/Computers/Groups/OUs.
58. Solution must be able to audit GPO changes, verify its consistency & also compare GPO version side- by-side.
59. Solution must have provision to revert the GPO changes.
60. Solution must have capability to test pre-production GPO clones before rolling them out.
61. Solution must have option to define a list of GPO settings with predetermined values that must exist and cannot be modified.

62. The Solution should be able to effectively administer and control Group Policy Object (GPO) changes and verify, compare, update and roll back GPO versions. Ability to confirm the consistency of various GPO settings.
63. Solution should have capability to integrate with AD to centrally create, modify, and manage the GPOs. Link the GPOs to users/Computers/Groups/OU's.
64. Solution must lock a GPO and prevent it from being edited.
65. Solution should be able to monitor changes to GPOs and creates a new version.
66. Solution should have self-service portal for password resets of AD and to unlock the account on their own.
67. The Solution should be able to provide a simple, secure, self-service solution that allows end users to create AD ID, reset forgotten passwords and unlock their accounts.
68. Self-service password management for on-premises AD.
69. Self-service password reset portal should be integrated with Multifactor authentication to use SMS, Email, and Smartphone Push Method.
70. The bidder has to install, commission and manage Microsoft ADFS (Active Directory Federation Services) solution in the Bank. Bidder has to provision Microsoft Services for installation of the same.

## **ENDPOINT and PATCH MANAGEMENT**

1. Proposed patch management solution must offer all the patching, application/ software delivery, license metering and asset inventory management capabilities, for Windows and non-windows operating system. The solution should patch all the flavours of Windows client OS (Windows 10 and above and all future versions), all flavours of Windows Server OS above 2016, RHEL Linux Server OS, Other Linux flavour, Guest OS in VMs (Using any hypervisor like VMware / Nutanix). All critical application/software must also be patched as soon as patch/upgrade is available. Solution must support Intel and AMD CPUs both x86 and x64 architecture.
2. Proposed solution should do granular filtering of software patches based on environment requirements.
3. Proposed solution should identify, schedule, deliver and track operating system and automate patch delivery.
4. Proposed solution should provide end-point security with automated OS and application patch management.
5. Proposed solution should remedy vulnerabilities and enforce security policies.
6. Proposed solution should schedule periodic scans computers to identify missing patches
7. Proposed solution should identify and download missing patches from vendors' websites
8. Proposed solution should download required patches and create tasks to schedule patch deployments
9. Proposed solution should be supported for deployment of patches at end-points and servers

10. Proposed solution should provide industry recognized vulnerability scanning and reporting for the purposes of integrated remediation of non-compliance
11. Proposed solution should have bundled reporting software so no third party tools would be required to customize reports
12. Proposed solution should be able to provide audit reports.
13. Proposed solution should be capable of providing Asset Management List with details of all the Hardware and/ or software installed on Bank's network as and when required by the Bank.
14. Proposed solution should be capable of integrating with one or more Active Directory structures whenever required
15. Proposed solution should have the ability to throttle bandwidth. The throttling capability must support down- stream throttling for both the server and agents
16. Proposed solution should be capable of using a system as distribution points at remote sites.
17. Proposed solution should support centralized architecture.
18. Proposed solution should be able to deploy patch management agent as well as the patches with the help of IP addresses / host name.
19. Proposed solution should have the ability to do centralized patch management for PCs, Servers, mobile device like Laptops and Surface Device.
20. Proposed solution should be able to install package through following mechanisms:  
Push Pull User self-service
21. Proposed solution should support virtualized environment
22. Proposed solution should provide remote agent deployment utility for installing agents remotely. The tool should be able to use Active Directory or Local Administrator Authentication for deploying agents to remote computers
23. Proposed solution should provide easy to use in-place upgrade procedures for all components through the console
24. Proposed solution should have native support for high level of encrypted communications
25. Proposed solution should support centralized administration, role-based access control and administration without much load on the network
26. Latest fixes/ updates should automatically be downloaded to the patch management server on the same day that the patch is made available on software vendors' websites.
27. All the patches downloaded must be applied to the endpoints (all devices like servers, laptops and PCs) after successful testing to avoid any disruption in services.
28. There should be a UAT set-up where every patch is to be tested before actual installations at endpoints or servers.
29. If any information or payload (e.g. Patch Metadata or Patch binaries) is downloaded from internet, then the integrity of all such content must be verified by the proposed solution using checksums to ensure that the content downloaded has not been modified or corrupted. File checksums and file sizes must be compared to make sure that the downloaded file is intact and unchanged
30. Proposed solution should be able to determine if a patch has already been installed on a node, even though it is assigned manually. Proposed solution should have the



- capability to analyse appropriate patches of the OS/ applications for the Desktop/ server in comparison to the latest available patches/ updates released by respective OEMs
31. Proposed solution should be able to detect the required patches according to individual node's configuration
  32. Proposed solution should allow users to postpone the deployment of a patch for a period of time determined by the administrator
  33. Proposed solution should support rollback of patches and service packs applied on windows system.
  34. Proposed solution should have the capability for remediation i.e. continuously deploy, monitor, detect and enforce patch management policies
  35. Proposed solution should support easy integration with enterprise Wide area Network (WAN) i.e. providing vulnerability assessment, device discovery etc. as per the IP address/host name/ domain
  36. Proposed solution should be able to deploy any software/ files through the patch management solution
  37. Proposed solution should have the capability to generate report specific to one group of servers/endpoints or should be capable of generating reports with an enterprise view
  38. Proposed solution should be able to verify if the patches on desktop are correctly installed by confirming that the vulnerability has been remediated
  39. Proposed solution should come along with standard reports and should generate customized reports as per business requirement
  40. Proposed solution should support various reporting formats i.e. reports can be downloaded easily and or exported
  41. Proposed solution should have the ability to consolidate scan data and to produce a single report for the entire network.
  42. Proposed solution should support regulatory specific reports i.e. reports required by the regulators as per the format shared by them during audit.
  43. Proposed solution should be able to dynamically group computers/manually group computers together for deployment of patches.
  44. Proposed solution should be able to re-deploy the patch on a computer automatically if the initial deployment is not successful and even if the deployed patch is un-installed by the user
  45. Proposed solution should support granular control over re-boot process after patch deployment like prompting user, allowing user to differ, rebooting immediately if no one has logged on, etc.
  46. Proposed solution should come along with all operational technical manuals along with other related documents
  47. Proposed solution should be able to identify the computers that have installed the patch that is to be rolled back on need basis and rollback updated patches on need basis.
  48. Proposed solution should be able to provide real-time (within minutes) patch deployment status monitoring
  49. Proposed solution should allow console operator to deploy patches to all computers via a central console without intervention from the users or allow console operator to target which computers to deploy the patches to.

50. Proposed solution should allow console operators to spread the patch deployment over a pre-defined period of time to reduce overall impact to network bandwidth
51. Proposed solution should be capable of generating reports on patches deployed, when, by whom, to which endpoints, etc.
52. Proposed solution should be able to identify systems with non-patched vulnerability conditions
53. Proposed solution should allow the console user to deploy actions to remediate against the vulnerabilities identified
54. Proposed solution should have the dashboard to drill down to show details for both compliant and non-compliant systems.
55. In the proposed solution, information reported should not be more than 1-7 days old for devices that are active on the network
56. The reporting module should contain, but not limited to, the following reports: (i) Progress of all patches applied (ii) Patch Compliance report for selected month /System (iii) Patch Compliance report for single patch (iv) Number of vulnerabilities detected by month; (v) Total number of computers managed and the distribution of these computers;
57. Proposed solution should allow to export report in CSV, PDF & XLS format.
58. Proposed solution should allow to customize and save the reports without the use of third party reporting tools
59. Proposed solution should allow to drill-down from the report to the specific computers
60. Proposed solution should allow to trigger alerts when user defined conditions are met e-mail and SMS based alert system.
61. Proposed solution should generate both pre-packaged and custom, wizard generated reports like compliance reports can be generated for one month patches or one particular patch on all system or on one system.
62. Proposed solution should be capable of software distribution and installation e.g. Chrome, MS Office, Antivirus agent, drivers etc. in silent mode. It should support software distribution on Windows and Linux Systems.
63. Proposed solution should have automatic patch management and deploy patches for various platforms including Windows and Linux as per RFP
64. In the proposed solution reports should be scheduled to be run and sent to administrators at specified times and intervals
65. In the proposed solution, reports should be viewed online
66. In the proposed solution, reports should be downloaded in CSV/ PDF/ XLSX formats as per requirement of the Bank.
67. The proposed solution should support proper business continuity plan.
68. Vendor should provide interface to integrate to multiple monitoring and reporting tools. Integration with SIEM should be supported
69. Bidder should provide updates, patches, rollups for all software supplied including operating system and should update the same immediately after its release. Back to back OEM support for all Software and updates to current Version is required to be provided. OEM authorization, partner status and back to back support document is to be submitted as part of eligibility bid.

70. All critical patches for all software supplied should be applied to end points within 15 days or as per the recommended timeline (whichever is lower) mentioned by OEM of release of critical patches.
71. Solution should be able to push, Install and uninstall any file/certificate to/from target system in a hassle free manner.
72. Prevention against unauthorized installation of software and unauthorized external devices e.g. USB, HDD etc. The solution should provide Blacklisting and Whitelisting of Software from the central location. Application whitelisting and blacklisting.
73. Remote software installation allowing for more timely software upgrades, patches and updates.
74. Automatic security Patch management and centralized license management.
75. The solution should be capable of automatically accepting new software/application added which are already whitelisted through policy for connected and disconnected endpoints for Application Software Control.
76. The solution should be automatically push policy on systems.
77. The solution should be capable to update the existing applications on the client machines only through a trusted process/installer/hash or user.
78. The solution should be able to define specific policies for specific sets depending upon the requirements.
79. The solution should augment blacklisting as per requirements.
80. The solution should ensure that only authorized software is allowed for installation.
81. The solution should have a small overhead footprint which includes:
  - i. Easy setup and low initial and ongoing operational overhead.
  - ii. No file system scanning that could impact system performance.
  - iii. Designed to work in disconnected and in "offline" mode.
82. The solution should cover cases where the name of the application/application's exe is changed by the user.
83. The solution should offer control over the applications, based on the information of the Applications.
84. The solution should update the whitelisted applications locally and dynamically when trusted and authorized changes are implemented. The solution should be capable to maintain whitelisting records locally so that it works in offline mode as well.
85. The solution should allow only authorized applications to run.
86. The solution should be able to work in monitoring as well as blocking mode.
87. The solution should give granular control to block versions.
88. The solution should be capable to support systems having with least resource consumption (i.e. thin clients having min 4 GB RAM, 40 GB HD with Windows 10 or later OS etc.)
89. The solution's management console should be web based / Client based and should use Active Directory accounts and groups to manage roles.
90. The solution's management console should provide for separation of functions and access by roles.
91. The solution should provide pre-defined common reports and customizable reporting.

92. The solution Client should be capable to co-exist with all the major Anti-Virus Solution like Symantec, McAfee, Trend Micro etc. and other end point clients like DLP etc.
93. The solution should be integrated with SIEM Solution and able to generate alerts by the SIEM.
94. The solution should be capable to provide fault tolerance when the primary data centre is down.
95. System shall be deployed for high availability at DC and DR Site and Data should be replicated between DC and DR Site. The Solution should have capabilities for Auto Sync for the DC and DR Location with same level of security.
96. DR site should be made identical to DC.
97. The Solution should automatically accepts new software added through authorized process.
98. The Solution should be capable to deploy the policies in scheduled process or real time basis.
99. The solution should support Process Blocking through Kernel and Driver level Blocking.
100. Solution should support Permanent Trusted Level- Allows applications that match this rule to install and start any other applications.
101. Solution should support all the Browsers and their versions.
102. Solution should have capability to set up approval workflow or should have option for multi-level administration.
103. The solution should be capable for Capturing User Activities logs including administrator activities.
104. The solution should be capable for alert monitoring dashboard generated for blocking any application on endpoints.
105. The solution should be able to block any application by Name, path and Hash Value.
106. The solution should be able to block application in learning mode/after installation of agent also.
107. The solution should be able to work in case of OS version Upgrade and agents should be upgraded automatically.
108. The solution should be able to show the blocked application details of endpoints on dashboard.
109. The solution should be able to learn the applications within minimum time.
110. The solution should be able to push the policies to all the endpoints and able to re-push in case of failure. The solution should be able to provide the reports for pushing details like start to time, end to time, user details, status etc.
111. The solution should have the capabilities that no user is able to stop/disable the agents in endpoints.
112. The solution should not have any negative impact of Operating system files/Driver files in endpoints.
113. The solution or its agent should not create unnecessary network traffic or load on the target servers/clients/network link.
114. The solution agent should consume minimum resources like CPU/RAM/Disk space in endpoints/servers.

115. The solution should have the capabilities to provide the dashboard and report for non-communicating agents installed in endpoints.
116. The solution should be able to provide the report for policy applied on all the endpoints.
117. The solution should have the capabilities to backup/restore the data as per Bank retention policy.
118. The solution should provide ability to setup remote access for Windows/Linux based server/workstations.
119. The solution should maintain audit logs for remote access sessions
120. The solution should provide option to record remote support session
121. Only permitted users should be able to take remote desktop of the End user for troubleshooting, maintenance and training purposes
122. The solution should have capability to store all the audit logs like session recording, activity log, day, date, time and duration of access, Administrator name, IP address etc.
123. The solution should have capability to get the User confirmation prior taking the remote session and Administrator should have the capability to bypass or revoke the user confirmation prompt.
124. The Solution should be able to list all Hardware, software and applications, including version numbers, which are installed on the agent.
125. The Solutions must provide device network discovery and inventory of all hardware and software connected to network, including computers, servers and non-computing network devices. The support platform must include, but not limited to Windows, Mac, Linux, Chrome OS etc. Should also Discovery VM's and its resources by integrating with Hypervisor
126. The Solutions should allow to import offline asset inventory
127. The Solutions should be capable of Asset allocation to single user, Asset allocation to multiple users, Asset allocation to project, Asset allocation to department, Asset allocation to location, Bulk Allocation of Assets, Asset Return & Re-Allocation process
128. Assets profile need to be done on the basis on unique identifier
129. The proposed solution should consolidate end-to-end lifecycle management of IT hardware and software assets.
130. Proposed Solution should be capable to reattempt the failed patches automatically and able to generate reports for the same.

### **Patching of Redhat Linux on s390x Platform Servers and Solaris Sparc Servers**

Bidder has to supply, install, configure and manage the Patch Management solution for patching Red Hat Enterprise Linux 8/9(RHEL 8/9) Operating System on IBM LinuxOne Z Systems with S390x Architecture and Solaris Sparc Servers. The patch management solution must have Discovery and Assessment for patching servers, Solution Design and Planning, Solution Implementation and Configuration, Deployment and Rollout, Post-Implementation and Ongoing Management, Training and Knowledge Transfer. It would be Successful Bidders responsibility to Patch the Servers as per Bank's Patch Management Policy. The

patching process should not hamper the operation of the Servers due to High utilisation of CPU and RAM.

### **SFTP SERVER**

1. Bank is looking out for a solution that ensures reliable, secure and manageable file transfer across the enterprise and outside (internet).
2. The solution should be fully standards compliant and scalable and ideal for businesses of all sizes.
3. The Bank is considering to procure a solution which will eliminate the problems of managing file transfers and enabling secure and robust file transfers.
4. The solution should support the Bank to keep track of file movement and ensures confidentiality, integrity and authenticity of information.
5. The solution should be platform independent, easy to incorporate and cost effective to deploy.
6. Should not require integration of any standard/proprietary technologies with the application servers
7. Solution should ensure that no re-engineering of business applications is necessary.
8. The Bidder is required to Supply required Software Application with required licenses, install, configure & deploy the solution at the Bank's Datacenter and DR site, provide training by OEM and migrate the existing SFTP, FTP setup to the proposed SFTP Solution. The Bank would supply hardware and OS (Windows / Redhat Linux). Oracle Database license where required would also be supplied by the Bank. The bidder has to install and maintain the Operating System, Database and application Software.
9. System shall be deployed for high availability at DC and DR Site and Data should be replicated between DC and DR Site. The Solution should have capabilities for Auto Sync for the DC and DR Location with same level of security.
10. The bidder has to perform DR Drill of the solutions.
11. DR site should be made identical to DC.
12. Solution must support HA for both Client and Central Hosts Deployment
13. The bidder is expected to provide the solution including implementation, testing, migration, installation, providing requisite interfaces, training and to provide technical support for a period of 5 years.
14. The bidder should provide the complete documentation including technical, operations, user manual, design documents, process documents, technical manuals, functional specification, system configuration documents, system/ database administrative documents, debugging/ diagnostics documents, test procedures etc.
15. If there is any upgrade to the source systems such as CBS etc., then it will be Vendor's responsibility to ensure that appropriate integration is provided without affecting the normal course of business.
16. The ATS support for SFTP Solution should include the following:
  - i. All minor and major version upgrades during the period of contract at no extra cost.
  - ii. Program updates, patches, fixes and critical security alerts as required.
  - iii. Documentation updates.

- iv. Call basis Support for Solution related malfunctions, configuration as defined in SLAs and ability to log requests online. If required, OEM Engineer may have to visit the site for resolution of the issue.
- 17. The price quoted by the bidder should cover all the support to the solution including any updates/upgrades and fixing any issues faced. Bidder should provide onsite support to fix the issues for the period of 5 Years.
- 18. The bidder should comply with the Bank's Information Security policy in key concern areas relevant to the RFP. Some of the key areas include (but not limited to):
  - i. Responsibilities for data and user privacy and confidentiality
  - ii. Responsibilities on system and software access control and administration
  - iii. Data Encryption/Protection /XBRL requirement of the Bank
  - iv. Protect information from unauthorized modification or destruction
- 19. Any planned downtime for SFTP Solution maintenance/ upgrade must be communicated to the Bank 30 days in advance. No data loss should occur during the maintenance/upgrade.
- 20. Vendor must provide an alert service for any problems with the service being unavailable. This can be in the form of SMS and E-Mails and should be sent to designated persons.
- 21. Any level or version changes, clarification, corrections and modifications in the above mentioned documents should be supplied by the bidder to the Bank free of cost in a timely manner.
- 22. The SFTP System should support online/ real-time comprehensive and customizable management dashboard.
- 23. The Solution should provide RBAC and audit logs should be captured.
- 24. The Solution should be integrated with Banks Active Directory for Authentication.
- 25. Solution should have capability to assign size of the folder per user.
- 26. The solution provides Server to Server File Transfer.
- 27. The solution should be able to integrate with SIEM and SOAR Solution
- 28. The solution should be integrated with Banks Active Directory.
- 29. The licenses for SFTP Solution should be perpetual.
- 30. Installation of the Solution should be done by OEM/OEM authorized Engineer.
- 31. The proposed solution should support both IPv4 and IPv6.
- 32. Bank will perform its own Vulnerability assessment/ Penetration testing (VAPT) & Risk assessment on the entire solution before going live and the solution provider needs to fix all the vulnerabilities/risks highlighted in the reports at no extra cost to Bank.
- 33. There shall be a provision for taking backups and archive the replica of the systems' database and the application as well. There should be a provision of adequate Business Continuity Plan (BCP).
- 34. The Application should have a capability for easy retrieval of the backed-up data (both application and the database) with least amount of manual intervention with no data Loss events.
- 35. There shall be provision for complete audit trail of all operations by the users. There shall be provision / functionality to track down all backend modifications as per assigned users' roles and responsibilities if any, by any user, which can be retrieved

and analysed to get the complete history of the issue. The vendor may take it as an input for redressal of the issue, if the same is application related.

36. Solution should provide for a Central Host to transfer files with Clients Hosts securely, while preserving file format and its integrity.
37. Solution should provide simple and minimal process for on boarding Client Hosts.
38. The solution should ensure file transfers only between authenticated hosts. Strong authentication mechanism should be supported, preferred model is mutual authentication using digital certificates.
39. Solution should support multiple channels to send or receive files - HTTPS, SFTP, File System
40. The exchanging files between Central host and client host could be uni-directional or bi-directional. The Solution should provide facilities for configuration based on Host's preferences.
41. The Solution should provide option to configure patterns to rename files as per the configured rules
42. The Solution should ensure the file integrity is checked for file transfers, preferably through digital signatures.
43. The Solution should have ability to encrypt files before transfer initiates and decrypt once transfer is complete. The option to encrypt/decrypt should be configurable at Host level. Should have an option of using industry standard encryption/decryption methodology (PGP, AES, 3DES).
44. The Solution should have ability to maintain multiple folders for pickup and delivery of files from Client to Central Host and vice-versa
45. The Solution should provide mechanism to check duplicate files based on file content, file name or both
46. The Solution must employ mechanisms to check for incomplete files
47. The Solution should have ability to specify daily time range between which transfer is allowed for prioritized Clients
48. During file transfer failure, the Solution should have ability to resume file transfers from the last failure point instead of reinitiating complete transfer.
49. The Solution should have ability for automatic retries for file transfer in case of failures
50. The Solution should be capable to send/receive large files (in GBs)
51. The Solution should have ability to transfer files where there are proxy level settings at Client hosts
52. The Solution should have abilities for alerts and notifications by way of email/SMS
  - a. Failure to transfer files after retries
  - b. Acknowledgement alerts for successful transfers
  - c. System failures
53. Solution should be capable to monitor continuously and send intimation alerts to the configured users
54. The Solution should offer Client host management Dashboard for real-time monitoring
55. The Solution should provide control to centrally manage the Client Hosts from master host. The solution must be able to cater to :



- i. Client Management - Enrolling/Removing, Updates, Fetching details, Certificate renewals
  - ii. Health Check-up - Continuous feed whether the clients are active or dormant
  - iii. Upgrades - Provision for automated or manual triggered process for applying product patches/updates/upgrades
  - iv. License - Upgrades/Renewals must occur from central location
  - v. Failure alerts - Configure the failure points for alerts - based on the criticality, including client profiles
56. Any other features in addition to the above mentioned that will help in smooth running of day-to-day activities will be considered for qualification
57. Solution should support for bulk update of Client Hosts from Central Host
58. Solution should offer Dashboards - Common report interface for providing the admin activity, transaction report and system logs
59. The Solution should provide easy to use web-based administration panel
60. The Solution should provide a GUI for managing multiple Admin users. Authorized Officials should be able to login to this web based platform and be able to create and manage Admin users.
61. The solution should implement strong access controls and authentication measures. It should have ability to provision granular access control and shall support monitoring and logging of access.
62. Solution should support dual-authorization model while approving state changes in the system
63. Solution should support configuration for various events including status of Client hosts
64. The Solution should have the capability of detailed logging and audit tracking of all key state changes, administrator access and policy changes.
65. The Solution should have facility to maintain logs for file transfers for reporting and tracking purposes. The reports should be exportable with/without appropriate filters
66. The Solution should be compatible with standard operating systems such as Windows, Linux/Unix

## **OPERATING SYSTEM –REDHAT LINUX VDC LICENSES**

Bidder has to supply and install the Operating System licenses for Red Hat Linux VDC.

## **LOAD BALANCER**

Bidder has to supply, install, configure and maintain the Load Balancers in the Bank at DC and DRC Sites during the Contract Period.

## **ANTIVIRUS**

1. Bank wants Antivirus Solution for its Systems working on Internet.
2. Bidder has to supply the licenses and install the Management Servers at DC and DR location in such a way that the Systems on internet can be managed for policies and updates.
3. The Management solution should be installed at Bank's DC and DRC location and Cloud solution is not allowed.
4. The successful bidder has to manage the solution during the contract period.

**AMC support for Oracle T8-1 Server for 5 years as mentioned in the Annexure 2: Commercial Bill of Materials.**

**All the configurations have to be done by the OEM / OEM Certified Engineer.**

#### GENERAL TERMS

1. The selected Bidder should create SOPs.
2. Bidder to ensure that no software reaches end of life or end of support during the entire contract period, failing which, bidder will be required to upgrade or replace the same at no additional cost to the Bank.
3. Bidder is required to provide RCA for all key issues for the in-scope applications within 24 hours of the issue being identified/ notified.
4. Vendor should have to perform/configure backup for all the supplied solutions/applications as per Bank's policy/requirement.
5. The Successful bidder is expected to ensure that all statutory and regulatory changes for the entire contract duration of the respective solution is incorporated in the solution at no additional cost to the Bank.
6. The AD Management Software solution, Endpoint & Patch Management Solution and SFTP Solution shall include all commercial licenses for app, database, middleware, etc. as required for the functioning of the solution. No freeware or unlicensed open-source software should be used in the solution. All the Licenses should be enterprise class.
7. Successful Bidder will provide knowledge transfer/ training to Bank team/ staff & SI prior to completion of the installation and commissioning of Solution.
8. Bidder should conduct preventive maintenance on quarterly basis.
9. Project documentation along with SOP for each activity in detail should be submitted.
10. Vendor will provide a detailed formulated project plan, architecture with timelines for the implementation of the infrastructure in hard copy as well as in soft copy
11. The Bidder should have premium support arrangements with the respective OEM. The successful bidder should have back to back agreement with the OEM for troubleshooting, patching, support through call centre or customer web portal and any other services which Bank is entitled to obtain from the OEM. The Bidder and Bank should be able to log a call with the OEM directly.
12. The bidder should submit the future roadmap of at least 5 years of the respective OEM regarding development and support of proposed solutions/ products.

13. The successful bidder shall handle all matters including the configuration, implementation, operation, monitoring, management and maintenance of the proposed solution.
14. Bidder must have valid licenses and ATS contract with the OEM for all the Software used to implement the proposed solution.
15. The hardware and software supplied by the vendor should be of latest versions and should reach end of support/ end of life only after 7 years from the date of supply. The technology providers, including OEM will be required to submit a written undertaking, explicitly stating their commitment to provide spares, full technical, operational and maintenance support to Bank during the warranty and AMC period.
16. All Software must come with 1 years of warranty and 4 years of AMC/ATS post completion of warranty period. There should be provision of extension of AMC/ATS for a further period up to 2 years at the 5<sup>th</sup> year cost.

#### INSTALLATION and SUPPORT DURING CONTRACT PERIOD

1. The installation will be done by OEM. The bidder has to provide at least two technical experts from OEM during implementation. After commissioning the bidder has to provide onsite one Resource for (Active Directory Management and Endpoint & Patch Management) for technical support without any additional cost such as travelling, lodging during the contract period as per the commercials sheet in FM Resources.
2. The technical resources should be competent to handle/ integrate/ implement/ test/ go-live of the solution/customizations within Bank's stipulated time. Onsite resource is expected to perform, testing, UAT, preparation of test cases, support, monitoring, certification, implementation, reporting, coordination with Banks team/s, Audit compliance, VAPT(Vulnerability Assessment & Penetration Testing) closure, any other statutory compliance, patch installation, fixes, analytics, logged complain for software/hardware issues, day to day MIS reports, conducting DR Drill, DC-DR Drill, database support including performance monitoring, perform daily/weekly/monthly/yearly backup and restoration activity, optimization, maintenance of table spaces, log files, troubleshooting, online replication with zero lag, product documentation, user management and post go-live support. Detailed process documentation, SOP (Standard operating procedure) and management of solution should be created and submitted. Selected bidder is expected to deploy OEM resource who is academically good, technically sound and competent personnel to ensure smooth operations at Bank's site. The deputed personnel will be employed by the selected bidder on OEM payrolls/ contracts without having any employment right with the Bank. Moreover, deployed personnel will not have any right whatsoever to lodge claim of any nature directly or indirectly with the Bank and it would be responsibility of selected bidder to address such issues without involving the Bank. The deputed persons have to maintain the utmost secrecy & confidentiality of the Bank's data including process performed at the Bank premises. At any time, if it comes to the notice of the Bank that data has been compromised/ disclosed/ misused/ misappropriated then Bank would take suitable action as deemed fit and selected vendor would be required to compensate the Bank to the fullest extent of loss incurred by the Bank. Bidder is expected to adhere to

- Bank's request for removal of any personnel, if Bank notices any negligence/gross misconduct/violation of trade secret/disclosure of Bank's data to third party and any decision of the Bank in this regard would be final and binding upon the selected vendor.
3. The vendor should provide a detailed description of how the updates/ upgrades will be reaching the desktops/ servers to update the OS Patches with reference to size of the updates, the frequency of updates and bandwidth utilization etc.
  4. Prices payable to the successful bidder as stated in the Contract shall be firm and not subject to any changes under any circumstances during the contract period or period of deliverables under this contract whichever is later from the date of placing purchase order.
  5. The selected bidder has to do overall maintenance and working of the Patch Management Solution
  6. The selected bidder should fix the bugs and carry out the necessary rectifications wherever necessary and deliver patches/ version changes effected. Provision should be available for version control and restoring the old versions in case of need by the Bank.
  7. The selected bidder has to do Bug fixing, enhancement, modifications, customization, patches, upgrades due to statutory, regulatory, industry, Bank specific changes (including installation of new upgrades.)
  8. The selected bidder has to do configuration changes, version up-gradations, performance monitoring, trouble shooting, patch installation, running of batch processes, database tuning, replacement / support, technical support for application and data maintenance, recovery, query generation and management etc. of all software supplied under this RFP.
  9. The selected bidder has to undertake immediate bug fix actions in the event of software failure causing an interruption of operation of the Patch Management Solution as per the response / resolution times defined by Bank.
  10. The selected bidder has to notify all the detected software errors and correct them as per the agreed timelines.
  11. The selected bidder has to do routing of transactions through the backup system in case the primary system fails Switching to the DR site in case of system failure.
  12. Timeline for issue Resolution

Time from Issue Raised	Type of Support
Less than 2 Hrs	Issue must be addressed and tentative timeline for resolution must be provided.
After 2 Hrs upto 24 Hrs	Phone/onsite support if required by Bank, to be provided for resolution.
After 24 hrs upto 48 Hrs	Issue must be addressed with onsite support

13. No visiting cost will be provided by Bank
14. If selected bidder fails to resolve or does not attend the issue in mentioned time frame, penalty will be charged proportionately.
15. The successful bidder shall ensure that all the purchased licenses are active without any omission at any point of time. Bidder shall have constant follow-up to activate/ re-

install the licenses in case any system goes out of date and coordinate, follow-up in this regard, with the branches/ offices where such endpoint system is located.

#### **7.2.4 AMC/ATS for Hardware and Software Items**

1. The scope of the services and maintenance is to be provided for a period of five (5) years from the date of acceptance of installation by the Bank (i.e. 1-year warranty followed by 4 years AMC/ATS post warranty for Software and 3-years warranty followed by 2 years AMC post warranty for Hardware.). After expiry of Five years, Bank has the option to extend AMC/ ATS for additional two years at the same cost of 5<sup>th</sup> year price.
2. The bidder should keep the Bank explicitly informed about the end of support dates of the related products/hardware and should ensure support during the warranty and AMC period.
3. The bidder shall provide perpetual licenses and the Bank is free to procure AMC/ATS for all or part of the licenses provided in this contract.
4. The bidder shall ensure all kinds of maintenance, deployment, re-deployment of Solution under RFP scope, at central or remote sites and at endpoints of branches/offices as part of maintenance only. No additional charges shall be payable for redesigning / re- deployment or maintenance of solution at any or all endpoints including DC and DR sites of the Bank ordered from time to time. The bidder shall ensure all activities pertaining to continuity of the smooth running of the solution as part of AMC/ATS without any extra cost to the Bank.
5. Onsite Comprehensive maintenance of all applicable products, services, modules and accessories on yearly basis and sensitization of the end user for avoiding upcoming hazards on a regular basis. The vendor shall share the preventive maintenance reports in digital form/soft copy and hard copies shall, on demand by the Bank. If any part / items / accessories of the delivered products are found non-working / defective (due to whatsoever reason) during preventive maintenance, the Vendor at no extra cost to the Bank will replace it. The PM reports of the delivered products shall be duly recorded in two copies and produced as and when required.
6. Call basis Support for Solution related malfunctions, configuration as defined in SLAs and ability to log requests online. If required, engineer may have to visit the site for resolution of the issue.
7. Bank has the option for extending the AMC/ATS of the in scope components for additional 2 years after expiry of the contract at the same cost of 5<sup>th</sup> year AMC/ATS cost of this tender.
8. During Warranty and AMC Period, it will be mandatory on the part of the supplier to attend and resolve break down calls if any, as per the parameters/ timeframe defined in the “ServiceLevel Agreement”. The Vendor shall be responsible for non-compliance of SLA, due to delayed replacement of defective equipment /faulty parts/ software upgrades.
9. The successful bidder will attend to all breakdowns (due to whatsoever reason) in the Equipment/Systems, rectify problems thereof, and replace the faulty components of the systems with serviceable components. Such replacements will be free of cost on exchange basis. In the event the maintenance/ repair of any unit is to be carried out at

any of the workshops, the Vendor shall make all arrangements for removal and transportation of equipment to the respective workshop and back to site at their risk and cost and will hand over the equipment in 100% working condition after repair/maintenance/rectification.

10. The Bank may procure & install new component(s) as a part of up gradation of existing system. In such cases, the original equipment (less new components) will continue to be governed by the AMC agreement and the new equipment(s) procured shall be covered under AMC on expiry of warranty period.
11. The Vendor will have to handover the system in 100% working condition on termination or at the end of the contract. Any breakdown call that has been reported before termination of the contract shall have to be corrected by the Vendor before handing over to Bank.
12. For on-site comprehensive maintenance of equipment, the tools, test equipment and fixtures etc. required (if any) for maintenance shall be provided by the Vendor only.
13. The Bank can terminate the AMC contract to the supplier of the equipment and discontinue the same due to performance issues by giving 90 days' notice.
14. AMC contract can be extended at the discretion of the Bank at the same rates after the expiry of the contract period.
15. Payment of support will be done as per calculation of the uptime, which is mentioned in the related clause.
16. The Bank, at its sole discretion, will enter into AMC.
17. Include all applicable Software Modules / Components items as applicable, indicated in the Price Schedule.
18. Bank at its discretion can terminate the AMC contract in whole or as part thereof with the Vendor and discontinue the same without citing any reason by giving 90 days' notice and applicable amount, on a pro-rata basis, for the service rendered shall be payable.
19. For the crucial issue hampering the working of entire system, the maximum response time for a maintenance complaint from the site of installation (i.e. time required for Supplier's maintenance engineers to report to the installations after a request call / fax / e-mail is made or letter is written) shall not exceed 4 (four) hours.
20. The Supplier shall ensure that faults and failures intimated by the Bank as above are set right within 6 hours of being informed of the same.
21. The bidder shall ensure re-deployment of Solution at central or remote sites or at endpoints as part of maintenance only. No additional charges shall be payable for re-designing / re-deployment of solution at any or all endpoints including DC and DR sites of the Bank. The bidder as part of AMC without any extra cost shall ensure all activities pertaining to continuity of the solution to the Bank.
22. AMC for System hardware and Software / off-the-shelf Software will be provided to the Bank as per the general conditions of sale of such software.
23. Both the bidder and OEM will be totally responsible for the maintenance, configuration and fault free operations of supplied infrastructure i.e., hardware, software and its maintenance during the warranty and post warranty (AMC/ATS period) period.
24. Any technical glitch/ issue in installed infrastructure of the solution (i.e., hardware and software, OS/DB etc.) should be attended on priority and should cover under warranty/AMC.
25. Clauses related to Version Upgrades/Updates

- i. The successful bidder should provide onsite support for all minor and major version upgrades, firmware upgrades in time for the devices and software supplied by the Successful Bidder from the Original Equipment Manufacturer (OEM) and during the period of contract at no extra cost.
- ii. Program updates patches, fixes and critical security alerts as required.
- iii. Documentation updates.
- iv. All regulatory / statutory changes should be done without any additional cost to the Bank.

26. Right to Use Defective Product

- i. If after delivery, acceptance and installation and within the guarantee and AMC period, the operation or use of the product is found to be unsatisfactory, the Bank shall have the right to continue to operate or use such product until rectification of defects, errors or omissions by partial or complete replacement is made without interfering with the Bank's operation.
- ii. Arranging for the replacement of defective equipment / faulty parts (due to whatsoever reason) of equipment's on time basis as per SLA and the necessary coordination with OEM for the same during the whole contract period.
- iii. **Service Level:** All defective parts/faulty Part shall be replaced at no extra cost. Replacement parts shall be new part from the same manufacturer(s). Whether a defective item or component is to be replaced or repaired shall be at the sole discretion of the Bank. In the case of a part, the defective part removed from the system will become the property of the selected firm.
- iv. **Response Time Maximum:** Response Time for Remedial Maintenance under the contract is measured in elapsed coverage hours from the time a service request is received to the time the vendor's customer engineer arrives at Bank Site. This contract provides maximum of 4 coverage hour's response time.
- v. **Response Time Maximum:**
  - If Response time < =4 Hrs then no penalty
  - If Response time > 4 Hrs but <=8 hrs then 2% of Monthly Contract Value of solution if it is under warranty else 2% of monthly AMC cost of solution for each disruption.
  - If Response time > 8 Hrs but <=24 hrs then 5% of Monthly Contract Value of solution if it is under warranty else 5% of monthly AMC cost of solution for each disruption.
  - If Response time > 24 Hrs then 10% of Monthly Contract Value of Solution if it is under warranty else 10% of monthly AMC cost of solution for each disruption.

27. Statutory and Regulatory Requirements:

- i. The solution must comply with all applicable requirements defined by any regulatory, statutory or legal body which shall include but not be limited to RBI or other Regulatory Authority, judicial courts in India and as of the date of execution of Agreement. This requirement shall supersede the responses provided by the Bidder in the technical response. During the period of warranty / AMC, Bidder should comply with all requirements including any or all reports without any additional cost, defined by any regulatory authority time to time and which fall under the scope of this RFP / Agreement. All mandatory

requirements by regulatory / statutory bodies will be provided by the bidder under change management at no extra cost to the Bank during the tenure of the contract.

#### **7.2.5 Audit Trail Requirement**

- 1) Audit logs reporting & analysis tool: Solution should be able to capture and display all events (either in sequence or by event type) in a simple, intuitive interface to understand the contributing events to an infection during the contract period of 5 years.
- 2) Store log data in a compressed manner, data must be stored in encrypted form and shall have features that support different retention/archival requirements for various logs.
- 3) Logs Integration
- 4) In case of Material Workload, all logs of assets related to Bank's subscription/ tenant should be integrated with the Bank's SOC.
- 5) All logs in case of Standard Workload hosted on premise/ cloud should be integrated with Bank's/ SOC/SIEM/SOAR.

#### **7.2.6 Bidder FM Services**

Bidder is required to provide FM Services for the following below mentioned components –

- 1) Active Directory Management Solution,
- 2) Patch Management Solution,
- 3) SFTP Solution,
- 4) Operating System,
- 5) Load Balancer

Refer to section 7.3 of this RFP for detailed Bidder's FM Services

Refer to start and end date in Annexure 2: Commercial Bill of Materials

#### **7.2.7 Delivery & Installation**

The Bidder must perform below activities to successfully deliver and install the in-scope component required for this project.

- 1) The bidder to coordinate with the respective Data Centre SPOC (DC&DRC) in respect of all the assignments relating to this particular RFP.
- 2) The bidder is responsible for delivery, transportation, transit insurance, of in-scope components of the RFP, insurance till acceptance by the Bank, installation/implementation and commissioning of In-scope Components at sites including integration, acceptance testing, documentation, warranty, annual maintenance.
- 3) Any delay in installation of the proposed in-scope components for whatsoever reasons should not entail in expiry of insurance and the same should be continued to be extended



up to the date of installation, acceptance and commissioning of the in-scope components and its associated licenses by the Bank.

- 4) The bidder shall be responsible for installation and commissioning and other related activities.
- 5) During the installation, the bidder shall check physical availability of items as per the Bill of materials. If any of the items are not delivered / not as per the specification etc., the bidders' representative/s at the site shall take immediate steps and ensure all the items are delivered so that the installation is not hampered.
- 6) The Bidder shall have to arrange for all testing equipment and tools required for installation and maintenance.
- 7) In case damage of the property owned / leased by the Bank during delivery and installation which is attributable to the bidder, bidder has to replace the damaged property at no cost to the Bank.
- 8) The bidder shall adhere to the service level specified in the RFP for the migration of the data from existing solution to proposed solution.
- 9) Bidder shall document migration Plan(s) and design using the validated data collected during discovery process, including definition of the migration methodology to be employed.
- 10) The bidder shall adhere to the service level specified in the RFP for the installation/implementation of in-scope components supplied by the bidder.
- 11) The Bidder should provide the necessary Power, Space, Cooling requirements for the deployment of Hardware for in-scope Applications.
- 12) The Bidder is required to provide the necessary pre-requisites to the Bank at least two weeks before the product delivery.
- 13) Bidder is required to co-ordinate with the CBS-SI for the installation of all Software Licenses
- 14) Bidder is required to submit a report/certificate from OEM confirming that the installation is in line with RFP requirements, Bank's baseline security policy and OEM's standard installation practices.

### **7.2.8 Maintenance**

The Bidder must perform below activities to successfully install in-scope Components of this RFP after successful migration of the data.

- 1) The Bidder shall provide the High-Level Document & Low-Level Documentation with As-is built documentation to the existing vendor.
- 2) Provide Knowledge Transfer to Bank throughout delivery of the Service, which includes a detailed overview on the implementation and configuration parameters and features and functionality of Bank's in-Scope components of this RFP. This should include a handbook about maintenance, management and housekeeping which shall be guiding document to Bank and or its appointed Bidder.

### **7.2.9 RFP In-Scope Activity Set**

This section describes the High-level activity list to be followed by relevant stake holders will complete the required activities in the following set:

Activity Set	List of Detail Activities
Kick-Off Meeting	Bidder will: <ul style="list-style-type: none"> <li>✓ Conduct a Kick-off Meeting with the Bank stakeholders to review the project Scope, Approach, Deliverables, Milestones, and responsibilities of both parties.</li> <li>✓ During the Kick-off Meeting, Bidder will exchange contact, procedural and schedule information with Bank</li> </ul>
Pre-Site Tasks	Bidder will: <ul style="list-style-type: none"> <li>✓ At least one week prior to commencing Service at the Service Location, Bidder will provide Bank with a Pre-site Readiness Checklist. Bidder will verify that the necessary prerequisites listed in the Pre-site Readiness Checklist have been completed. Checklist includes an inventory of Bank's environment included in the Scope of the Service.</li> <li>✓ Bidder will meet with the Bank to confirm logistics, such as user access and workspace, and identify any modifications to Bank's inventory in the Pre-site Readiness Checklist.</li> <li>✓ When the Pre-site Readiness Checklist is completed and verified by Bidder, Bidder and Bank will schedule the Service to commence at the Service Location.</li> </ul>
Handholding and Training	Bidder will: <ul style="list-style-type: none"> <li>✓ Provide Knowledge Transfer / hand holding to Bank's technical staff throughout the delivery of Service, which includes a detailed overview on the implementation and configuration parameters and features and functionality of the proposed in-scope Application software and System &amp; Supporting software.</li> <li>✓ A detailed training by Bidder/OEM has to be conducted for selected Bank employees / SI on the implemented solution</li> </ul>
Project Closure	Bidder will: <ul style="list-style-type: none"> <li>✓ Review the proposed Applications, System Software and supporting Applications with the migrated data with Bank's project team.</li> <li>✓ Review Service-related documents with Bank.</li> <li>✓ Review troubleshooting, support, and escalation procedures with Bank.</li> </ul>

#### **7.2.10 Mandatory Training/ Knowledge Transfer**

- 1) A Comprehensive training shall be the key to successful Operations and Maintenance; hence, the Bidder is required to provide required training to Bank nominated Officials. The training documents, including Operating Manuals, Standard Operating Procedures (SOP) for the proposed solution shall be prepared and shared by the bidder with BANK. Training will be conducted at Bank location for the batch of around 10

resources for 2 days in 2 batches for each module. The required infrastructure for training will be provided at Bank's location.

- 2) However, at a minimum, the plan shall include the following:
  - Overview of the components Installed
  - Technical Architecture
  - Technical and Operational Manual of the solution
  - Handling worst case scenarios (Malwares, Zero Day Vulnerabilities among others)
  - The above plan is only indicative; the final training plan shall be finalized between the successful bidder and Bank. No separate charges will be paid for training

### **7.3 Facilities Management Services**

- 1) This section describes the Facility Management (FM) services required by the Bank in the RFP. Successful Bidder needs to consider and envisage all services that would be required in the maintenance of in-scope components part of this RFP for the period of contract.
- 2) Facilities Management Services is envisaged for the DC, DR, Near Site, branches and offices including CO, ZOs, ROs and other administrative outfits. The support for branches and offices including CO, ZOs, and ROs will be provided remotely from DC and DR for the in-scope components of the RFP (hardware, software and application).
- 3) Facilities Management for all purposes means all onsite people deployed providing support, AMC, warranties, ATS required for the maintenance, monitoring and support of the application, and equipment.

#### **7.3.1 Facilities Management Services – Scope of Work**

- 1) Successful Bidder is required to provide support at all levels i.e. L1, L2, L3 for all in-scope components part of the RFP, during the tenure of the contract. Successful Bidder is required to provide branch level installation and remote trouble-shooting support for the components in the tender.
- 2) The FMS Engineer is required to provide support for equipment replacement.
- 3) The FMS Engineer is required to perform fine tuning for all the hardware equipment/Appliance and Software/System Software part of the RFP, on a regular basis.
- 4) The FMS Engineer is required to co-ordinate warranty repair or replacement service for the hardware and process warranty claims, as applicable.
- 5) The FMS Engineer is required to co-ordinate and schedule maintenance activities with the end user and appropriate support functions of the Bank.
- 6) The FMS Engineer is required to maintain accurate documentation on the current location and status of hardware/software in the process of being repaired /updated.
- 7) The FMS Engineer is required to provide maintenance data, as reasonably requested by the Bank, to support replacement/refresh scheduling.
- 8) The FMS Engineer is required to co-ordinate with all the stake holders including OEM for maintenance, replacement or any up-dation of software and agents.
- 9) The FMS Engineer is required to update, or provide the information required for the Bank to update the Asset Management system with the Bank.

- 10) The FMS Engineer needs to ensure that, any software patch updates / releases / advisory from OEM; OEM should notify Bank's stake holders via email and update the systems as per Bank Policy.
- 11) The Bank will not be liable to pay any additional amounts in respect of any sort of maintenance required during the tenure of the contract for in-scope components part of the RFP.
- 12) The FMS Engineer is required to provide preventive maintenance of in-scope components part of this RFP on bi-annually basis and submit observation reports to the Bank.
- 13) The FMS Engineer is required to conduct DR-drills quarterly as per Bank's schedule to test the functionality of the DR for the in-scope components in this RFP.

### **7.3.2 Scope of Work for Onsite Engineer / OEM Facility Management Engineer**

The Scope includes (but not limited to) the following:

- 1) Post go-live, on-site L1 or L2 support should be available during 24x7x365 days basis for the period of contract.
- 2) The Onsite resource should roll out and maintain all in-scope components part of the RFP.
- 3) Overall proactive monitoring through online dashboard and management of in-scope components and related services part of this RFP. The implementation of IT solutions on additional agents after signoff of the solution shall be done by onsite Engineer without any extra cost to the Bank.
- 4) Overall monitoring and management of the project during and after installation for the full period of contract.
- 5) Submission of periodical reports on the performance of all in-scope components and its reviews.
- 6) Redesigning of the solution for optimal output of the solution in interest of the Bank during the period of contract.
- 7) Prepare and maintain Standard Operating Procedure (SOP) document pertaining to the services/Operations.
- 8) The onsite resource should support and coordinate / cooperate with the Bank & vendor teams.
- 9) The onsite resource should optimize existing processes and recommend changes for optimal functioning of Solution, in-tune with best practices and audit compliance.
- 10) The onsite resource has to ensure the support from respective OEM for all in-scope components to carry out the activity for expansion, upgrade and configuration of proposed solution during the period of contract without any additional cost to Bank.
- 11) The bidder shall provide backup resource in case onsite resource avails leave.
- 12) Onsite resource should coordinate with all the internal teams for follow-up for open tickets & activities.
- 13) Confidentiality of the Bank's data and all related details shall not be disclosed by the bidder to any third parties or persons.
- 14) The Bidder should submit back-ground verification report of the onsite engineer along with all documents at the time of joining onsite.
- 15) The onsite resource to be deputed will be interviewed by Bank's officials prior to deputation. If not found as per Banks' requirement, Bank will not permit the deployment of such resource(s).

- 16) The deputed personnel should be prepared to work for extended hours in case of need.
- 17) The deputed personnel should abide by timings of the Bank.
- 18) The on-site resource shall not be changed without prior approval from the Bank and adequate notice period must be served i.e., minimum one month for L1 / two months for L2. Any resigned resource of the on-site team should not be relieved before giving suitable replacement; and should surrender/ submit all the Bank assets.
- 19) Absence of any resource must be complemented with an equally skilled resource.
- 20) If the onsite engineer is found to be not qualified / suitable / his performance is not satisfactory, the bidder will have to replace the engineer within 45 days of written communication from the Bank regarding the same.
- 21) The onsite resource should consult and assist various admin/application teams in operating and adapting to IT Operations management solution during the period of contract.
- 22) The resource should create Training/Knowledge Base (KB) Articles on the platform and associated tools and keep it updated timely as part of knowledge repository to enable self-learning with the Bank.
- 23) The onsite resource has to install, configure, manage, patch update version upgrade servers for Redhat operating System.

Any other task(s) associated/ related with the proposed solution and not listed above.

### **7.3.3 OEM Facility Management Scope for NUTANIX (L3)**

- 1) Management and Configuration of Hyper-Converged Infrastructure (HCI) lifecycle, Virtualized infrastructure management, Data centre migration planning and execution.
- 2) Ability to troubleshoot issues in nutanix environment.
- 3) Management and Configuration of Nutanix tools like Prism, Calm, Move and CLI tools.
- 4) Management and Monitoring of day to day operations of Nutanix solution and infrastructure.
- 5) Documentation and operationalization of Nutanix environment.
- 6) Application of Nutanix best practices and problem solving for compliance on Nutanix system.
- 7) Deployment and maintaining standards for Virtual machines.
- 8) Compliance of VAPT points.

#### **Administration**

- Installation assistance – VM Management/Cluster Management
- Patching and upgrades
- Daily Operations
- Self-Service Administration (create projects, configure roles, publish VM templates & images to catalog)
- Defining protection policies on critical VMs
- Creating and validating Recovery Plans
- Configuring Image Placement Policies
- Creating and Managing VGs (Volume Groups)

#### **Monitoring**

- Timely Health Checks
- Weekly progress reports

- Capacity planning and architectural strategy activities

#### Education

- Best Practices

#### **7.3.4 OEM Facility Management Engineer**

- 1) ACTIVE DIRECTORY MANAGEMENT SOLUTION -L3 RESOURCE of OEM/OEM Certified Engineer authorised by OEM.
- 2) ENDPOINT AND PATCH MANAGEMENT SOLUTION- L3 RESOURCE of OEM/OEM Certified Engineer authorised by OEM.

And

- 3) NUTANIX – L3 OEM RESOURCE is required.

#### **7.3.5 Service Window for Bidder and OEM Engineer**

Suitably qualified human resources shall be deployed to perform various activities under each of these service areas described in more detail further in this document.

Service Area	Services Window
L2 –In- Scope Solutions 1) Active Directory Management Solution, 2) Patch Management Solution, 3) SFTP Solution, 4) Load Balancer 5) Antivirus	24x7x365 at DC; for DR & NS (remotely from DC)
1. NUTANIX OEM L3 RESOURCE 2. ACTIVE DIRECTORY MANAGEMENT SOLUTION L3 RESOURCE 3. ENDPOINT AND PATCH MANAGEMENT SOLUTION L3 RESOURCE	On all Working days of the Bank 10 AM to 6 PM or as per requirement of the Bank.

#### **7.4 General Responsibility of the Bidder**

##### **Delivery, Installation and Maintenance –**

- 1) The Successful Bidder should co-ordinate with the respective SPOC (DC/DRC/Branches) for all in-scope components part of this RFP.
- 2) The bidder shall specifically mention the make and model of the items offered for all the requirements in terms of RFP without fail. Failing which the bid is liable to be rejected.
- 3) The bidder is responsible for delivery and installation of all in-scope components. The bidder should, also, be responsible for acceptance testing, documentation, warranty, AMC and ATS.
- 4) Any delay in installation and implementation of any in-scope component, for reasons solely attributable to the bidder, should not entail in expiry of insurance and the same should be continued and extended up to the date of installation and acceptance signoff for the delivered in-scope component and its associated licenses.
- 5) The bidder should be responsible for installation and other related activities such as unpacking, un-crating, post-delivery inspection etc.
- 6) During installation, the bidder should check physical availability of items as per the packing list. If any of the items are not delivered / not as per the specification / damaged etc., bidders' representative/s at the site shall take immediate steps and ensure all the items are delivered so that the installation doesn't get hampered. The bidder shall have to arrange for all testing equipment and tools required for installation, maintenance, and arrange the vehicle for transport at no additional cost to Bank.
- 7) In case of damage of the property owned / leased by Bank during delivery and installation of any of the components, which is attributable to the bidder, the bidder has to replace the damaged property at no cost to Bank.
- 8) The bidder shall ensure compatibility of to-be supplied software licenses with the hardware and software systems being used in Bank.
- 9) The bidder shall adhere to the service level specified in the RFP for the installation of software licenses supplied by them.
- 10) The bidder shall conduct preventive maintenance (including, but not limited to, inspection, testing, satisfactory execution of all diagnostics, cleaning and removal of dust and dirt from exterior of equipment and necessary repairing of equipment) at specified intervals as may be necessary from time to time to ensure that the equipment is in effective running condition so as to ensure trouble free functioning.
- 11) The bidder shall provide replacement component, if any component is required to be taken out of the premises for repairs at no additional cost to the Bank.
- 12) The bidder shall document the migration plan(s) and design using the validated data collected during discovery process, including definition of the migration methodology to be employed.
- 13) The bidder should ensure Knowledge Transfer to Bank throughout delivery of the service, which should include detailed overview of the implementation and configuration parameters and features and functionality of the proposed in-scope components.
- 14) The bidder is required to co-ordinate with Bank's existing System Integrator for implementation of OS on server hardware, VM creation, migration of data at DC & DRC
- 15) The bidder is required to co-ordinate with Bank's existing System Integrator for migration of database along with data from the existing server hardware to new server hardware at DC and DRC.

- 16) The bidder is required to co-ordinate with Bank's existing System Integrator for implementation of OS on server hardware at DC & DRC
- 17) All changes and/or customizations in in-scope proposed solution and AMC & ATS of in-scope components as and when required by Bank Officials, the same will have to be delivered at no additional cost to the Bank, during the tenure of the contract.
- 18) Data Validity and confidentiality: Bidder to ensure no unwarranted, illegal and fraudulent misuse of data shared by the Bank and bidder to categorically indemnify the Bank against any losses that the Bank may suffer on account of any such fraudulent and illegal act by the Company or its employees.
- 19) The Bank shall give Bidder/OEM and its personnel only physical access to the support location and the designated hardware & equipment to enable Bidder to provide the maintenance & support services. Any mode of remote access like VPN, Webex, Remote login etc. will not be allowed from any network outside Bank's Network
- 20) If the bidder feels that certain features offered are superior to what Bank has specified, it shall be mentioned separately. Information regarding any modification required in the proposed configuration to meet the intent of the specifications and state of the art technology shall be provided. However, Bank reserves the rights to accept the modification/ superior features suggested /offered.
- 21) The bidder shall provide all other equipment and services, whether or not specifically mentioned in the RFP, to ensure the intent of specification, completeness, operability, maintainability and upgradability.
- 22) The selected bidder shall own the responsibility to demonstrate that the product offered are as per the specification /performance stipulated the RFP and as committed by the bidder either at site or in bidder's work site without any extra cost to Bank.

## 8 Project Timelines

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

#	Activity	Weeks	Time Period for Completion
1	Supply and delivery of hardware components at DC, DRC	16 Weeks	Within 16 weeks of date of acceptance of the Purchase Order (PO) by the Successful Bidder
2	Installation of hardware at DC and DRC	8 Weeks	Installation and implementation of hardware and software, software licenses at DC and DRC solution - Within 8 weeks of date of delivery acceptance
3	Supply and delivery of software, software licenses at DC, DRC	6 Weeks	Within 6 weeks of date of acceptance of the Purchase Order (PO) by the Successful Bidder or Date of intimation by the Bank.
	Commissioning of Application / Hardware		
4	Active Directory Management Solution	24 Weeks	24 Weeks from the date of acceptance of the Purchase Order



#	Activity	Weeks	Time Period for Completion
5	Patch Management Solution	30 Weeks	30 Weeks from the date of acceptance of the Purchase Order
6	SFTP	14 Weeks	14 Weeks from the date of acceptance of the Purchase Order

The Bank, at its discretion, shall have the right to alter the delivery, implementation schedule and quantities based on the implementation plan. This will be communicated formally to the Bidder during the implementation, if a need arises. As there are many applications covered under this RFP, Bank will schedule the implementation plan and accordingly for some of the application above schedule will start from the data of intimation by the Bank.

## **9 Maintenance Support**

The Bidder must provide uninterrupted availability of the system and ensure that the problem is resolved within the time schedule as prescribed in the Service Level Agreement (SLA). For any major break down such as crash, the Bidder must arrange for immediate on-site support for recovery and resumption of operations. The re-installation of the software if required is the sole responsibility of the Bidder, which should be treated as service provided under. Maintenance support will also include installation of system updates and upgrades, providing corresponding updated manuals, and follow-up user training. During the ATS period, all upgrades should be free. All regulatory / statutory changes should be done without any additional cost to the Bank.

# **Section-3**

## **Terms & Conditions**

## 10 Liquidated Damage

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

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

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

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

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

## 11 Land Border Sharing Clause

The Bidder must comply with the requirements contained in O.M. No. 6/18/2019-PPD, dated 23.07.2020 Order (Public Procurement No. 1), Order (Public Procurement No. 2) dated 23.07.2020 and Order (Public Procurement No. 3) dated 24.07.2020. Bidder should submit the undertaking in Annexure17: Land Border Sharing Undertaking in this regard and also provide copy of registration certificate issued by competent authority wherever applicable.

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

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

- iv. An entity whose beneficial owner is situated in such a country; or
- v. An Indian (or other) agent of such an entity; or
- vi. A natural person who is a citizen of such a country; or
- vii. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.

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

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

### **Explanation**

- i “Controlling ownership interests” means ownership of or entitlement to more than twenty-five per-cent of shares or capital or profits of the company.
- ii “Control” shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder’s agreements or voting agreements.
- iii In case of partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more judicial person, has ownership of entitlement to more than fifteen per-cent of capital or profits of the partnership.
- iv In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more judicial person, has ownership of or entitlement to more than fifteen per-cent of the property or capital or profits of such association or body of individuals.
- v Where no natural person is identified under (1) or (2) or (3) above, the beneficial owner is the relevant natural person(s), who hold the position of senior managing official.
- vi In case of trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen per-cent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
- vii An agent is a person employed to do any act for another, or to represent another in dealings with third persons.

## **12 Monitoring & Audit**

Compliance with security best practices may be monitored by periodic computer security audits/Information Security Audits/Statutory and Regulatory audit performed by or on behalf of the Bank. The periodicity of these audits will be decided at the discretion of the Bank. These audits may include, but are not limited to, a review of: access and authorization procedures, backup and recovery procedures, network security controls and program change controls. The successful bidder must provide the Bank access to various monitoring and performance measurement systems. The successful bidder has to remedy all discrepancies observed by the auditors at no additional cost to the Bank. For service level measurement, as defined in SLA, data recording is to be captured by the industry standard tools implemented by the Successful bidder. These tools should be a part of the proposed solution.

### **13 Bid Submission**

- 1) Bidders satisfying the eligibility conditions (mentioned in Eligibility Criteria) and General terms and conditions specified in this document, may submit their bid through Government e-Marketplace (GeM) on or before the time-line stipulated in Invitation for Tender Offers.
- 2) All responses received after the due date/time be considered late and would be liable to be rejected. Government e Marketplace (GeM) portal will not allow lodgement of RFP response after the deadline. It should be clearly noted that the Bank has no obligation to accept or act on any reason for a late submitted response to RFP. The Bank has no liability to any Bidder who lodges a late RFP response for any reason whatsoever.
- 3) Bank will not accept the bid through any other mode except GeM.
- 4) Bid Security / Earnest Money Deposit: “Earnest Money Deposit” shall be paid through RTGS (Real Time Gross Settlement) / NEFT (National Electronic Fund Transfer) in the account no.-3287810289 of Central Bank of India (IFSC Code – CBIN0283154) with narration Tender ref no GEM/2025/B/6170727 in favour of “Central Bank of India” or by way of Bankers Cheque/Demand Draft/Pay Order favouring Central Bank of India, payable at Mumbai/Navi Mumbai.
- 5) The scanned copy of the receipt of making transaction is required to be uploaded on GeM portal at the time of “final online bid submission The RFP response without proof of amount paid towards Bid Security are liable to be rejected.
- 6) Guarantee of an equal amount issued by a scheduled commercial Bank (other than Central Bank of India) located in India, valid in the form provided in the RFP (Annexure 13: Bid Security (Earnest Money Deposit)). The Demand Draft should be of a Commercial Bank only (other than Central Bank of India) and will be accepted subject to the discretion of the Bank.

#### **Tender Schedule (Key Dates):**

The Bidders are strictly advised to follow the Dates and Times as indicated in the Time Schedule in the detailed tender Notice for the Tender. Ensure that no activity or transaction can take place outside the Start and End Dates and time of the stage as defined in the Tender Schedule.

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

### **14 Integrity Pact**

- Each Participating bidder/s shall submit Integrity Pact, as per attached Annexure
- duly stamped for ₹500 (Rupees Five Hundred Only). Integrity pact should be submitted by all participating bidders at the time of submission of bid documents or as per satisfaction of the Bank. The Non submission of Integrity Pact, as per time schedule prescribed by Bank may be relevant ground of disqualification for participating in Bid process. Hard copy of the Integrity Pact to be submitted to Bank prior to bid opening.
- Bank has appointed Independent External Monitor (hereinafter referred to as IEM) for this pact, whose name and e-mail ID are as follows:

- i. Shri Anant Kumar [anant\_in@yahoo.com]
- ii. Mr. Nirmal Anand Joseph Deva [mail: meghanadeva2022@gmail.com]

- IEM's task shall be to review – independently and objectively, whether and to what extent the parties comply with the obligations under this pact.
- IEM shall not be subjected to instructions by the representatives of the parties and perform his functions neutrally and independently.
- Both the parties accept that the IEM has the right to access all the documents relating to the project/procurement, including minutes of meetings.

## **15 Technical and Commercial Offers**

### **Technical Offer**

- 1) The Technical Offer (TO) should be complete in all respects and contains all information asked for, in this document.
- 2) It should not contain any price information. But a copy of the commercial bid without mentioning the price should be attached with Technical Offer (TO). However, any mention of price in Technical Offer (TO) will result in disqualification of the bid.
- 3) The Technical Offer (TO) must be submitted in an organized and structured manner. All the product brochures / leaflets / manuals etc. should be submitted along with the Technical Offer (TO). The technical offer should be in compliance with technical requirement / specifications.
- 4) The Technical Offer (TO) must contain the proof of submission of bid security. Without any of these two, bidder will be disqualified, and bid submitted by them will not be considered for process.

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

The Commercial Offer (CO) should be complete in all respect. It should contain only the price information as per Annexure 2: Commercial Bill of Materials.

- 1) The commercial offer should be in compliance with Technical configuration / specifications as per Annexure 12: Minimum Technical Specifications.
- 2) The price to be quoted for all individual items and it should be unit price in Indian rupees.
- 3) In case there is a variation between numbers and words, the value mentioned in words would be considered. The Bidder is expected to quote unit price in Indian Rupees (without decimal places) for all components and services on a fixed price basis, as per the commercial Bid inclusive of all costs. GST (Goods and Services Taxes) shall be payable as per applicable structure laid down under GST Law. The Bank will not pay any other taxes, cost or charges. The price would be inclusive of all applicable taxes under the Indian law like customs duty, freight, forwarding, insurance, delivery, and GST etc. Any increase in GST will be paid in actuals by the Bank or any new tax introduced by the government will also be paid by the Bank. The entire benefits/ advantages, arising out of fall in prices,

taxes, duties or any other reason, must be passed on to Bank. The price quoted by the Bidder should not change due to exchange rate fluctuations, inflation, market conditions, and increase in custom duty. The Bank will not pay any out of pocket expense. The Selected Bidder will be entirely responsible for license fee, road permits, NMMC cess, LBT, Octroi, insurance etc. in connection with the delivery of products at site advised by the Bank including incidental services and commissioning. Payment of Octroi, entry-tax, etc., alone, if applicable, will be made at actuals, on production of suitable evidence of payment by the Bidder.

- 4) The price is inclusive of taxes like Goods and Services Tax, which shall be paid as per actuals.

## **16 Evaluation & Acceptance**

- 1) Technical offers will be evaluated on the basis of compliance with eligibility criteria, technical specification, other terms & conditions stipulated in the RFP. Only those bidders who qualify in the technical evaluation would be considered for evaluating the commercial bid. Bank may, at its sole discretion, waive any non-conformity or deviations.
- 2) In case, any of the successful bidder is unable to honour in full or part of the contract awarded, Bank shall, at its sole discretion, distribute this shortfall to the other successful bidder(s) equally or in any ratio decided by the Bank.
- 3) Bank reserves the right to reject the bid offer under any of the following circumstances:
  - i. If the bid offer is incomplete and / or not accompanied by all stipulated documents.
  - ii. If the bid offer is not in conformity with the terms and conditions stipulated in the RFP.
  - iii. If there is a deviation in respect to the technical specifications of hardware items.
- 4) The Bank shall be under no obligation to mandatorily accept the lowest or any other offer received and shall be entitled to reject any or all offers without assigning reasons.

## **17 Evaluation Process**

The competitive bids shall be evaluated in three phases:

- Stage 1 – Eligibility Criteria
- Stage 2 – Technical Bid stage
- Stage 3 – Commercial Bid with Negotiations

### **Stage -1 Eligibility Bid**

Eligibility criterion for the Bidders to qualify this stage is clearly mentioned in Section 2 – Eligibility Criteria to this document. The Bidders who meet all these criteria would only qualify for the second stage of evaluation. The Bidder would also need to provide supporting documents for eligibility proof. All the credentials of the Bidder necessarily need to be relevant to the Indian market.

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

### **Normalization of Bids**

The Bank may go through a process of technical and/ or commercial evaluation and normalization of the bids to the extent possible and feasible to ensure that Bidders are more or

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

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

### **Stage-2 Technical Evaluation Criteria**

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

- 1) Compliance to the bill of materials as in Annexure 2: Commercial Bill of Material
  - i. The Bidder is expected to provide their "compliance" against each item stated in the Bill of material, this means that the Bidder confirms to the provisioning of the stated product / service and the terms of the RFP and subsequent addendums. Deviations to the Compliance requirements may lead to disqualification.
- 2) Compliance to the minimum technical specifications as in Annexure 12: Minimum Technical Specifications
  - i. The Bidder is expected to provide their "compliance" against each line item stated in the Minimum Technical Specifications, this means that the Bidder confirms compliance to the stated specifications and the terms of the RFP and subsequent addendums. Deviations to the Compliance requirements may lead to disqualification.
- 3) Bidder's detailed work plan – Bidder to share Gantt chart in conformity with the stated timelines. The Bidder should also share the key profiles and the number of representatives (across OEMs as well) being deployed across the Implementation Phase
- 4) Presence of Bidder Service centres in Mumbai and Hyderabad

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

- i. The bidder must comply to scope of the requirement as set out in the RFP and
- ii. The Bidder must comply to all the line items in Annexure 2: Commercial Bill of Materials indicated by The Bank as "(Bidder shall provide their compliance here)" in column "Bidder compliance (Yes/No)" Bidders are required to comply with the



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

- iii. The Bidder must comply to all the line items in Annexure 12: Minimum Technical Specification indicated by The Bank as "(Bidder shall provide their compliance here)" in column "Bidder compliance (Yes/No)" Bidders are required to comply with the requirements stated herein, if any Bidder's response is found to be non-compliant, then The Bank at its discretion may reject the Bid. Hence only the Bidders who have achieved the set compliance will be considered for commercial bid evaluation.
- iv. For the Solutions, Bank may at its discretion will do Site Visit and/or ask the bidder to do POC (Proof of Concept) and Solution Presentation of the tender components at Banks location and Bank has a right to disqualify Proposed Solution on the basis of same. For the POC bidder has to provide necessary Hardware and Software and its transportation at no cost to Bank. POC should be completed within 7 days of intimation to the Bidder to start POC for the Solutions.

### **Stage-3 Commercial Evaluation Criteria**

Only those Bidders who have qualified after Stage 2 of Technical evaluation will be eligible for the Commercial Evaluation Criteria .The total cost of ownership for the purpose of evaluation shall be calculated over the contract period of 5 years.

Bank will award the contract to the successful Bidder whose bid has been determined as the Lowest Commercial bid (L1) through the Procurement process of this commercial evaluation. Bank reserves the right to negotiate the Commercials with L1 Bidder, if required. At the end of 5 years, Bank has the option for extending the AMC/ATS of the in scope components for additional 2 years at the same cost of 5<sup>th</sup> year AMC/ATS of this tender.

The Total cost of Ownership of this tender will be the Grand Total - TCO quoted by the Bidder of the Summary Sheet of Annexure-2 Commercial Bill of Material.

The Bidder shall not add any conditions / deviations in the commercial bid. Any such conditions / deviations may make the bid liable for disqualification.

**Note:** Tendering process need not be cancelled merely on the grounds that a single tender was received provided that the single bid received is evaluated to be substantially responsive and deemed fit for award. Bank reserves right to proceed and award the tender to single bidder in case only one bidder participates in the tender / qualifies in the technical bid evaluation. Bank can negotiate with such single bidder, if required.

## **18 General Terms**

### **Payment Terms**

Payment will be released by the Central office from where the purchase order is issued. All the Payment shall be made in INR only. Payment terms are as under:

Item Description	Percentage Payment	Milestone
------------------	--------------------	-----------

Software  1. Active Directory Management Solution, 2. Patch Management Solution, 3. SFTP Solution and Others Software	60%	On delivery of Licenses
	30%	On Successful Installation & Commissioning of Application/Tool
	10%	3 Months Post Successful Commissioning of Application/Tool or Submission of equivalent amount PBG valid for 3 months
Software ATS	60%	On submission of documentary proof of “Back to Back Agreement with OEM” to Bank for renewal
	40%	Successful Upgradation to latest version of software and Sign off from Bank of Application / Tool
System Software (OS, DB, etc)	60%	On delivery of Licenses
	30%	On Successful Installation of System Software
	10%	3 Months Post Successful Implementation of System Software
Delivery of Hardware  Load Balancer	60%	On Delivery of Hardware/Appliance based solution
	30%	On Successful Installation of Hardware/Appliance based solution
	10%	3 Months Post Successful Implementation of Hardware/Appliance based solution
Installation & Commissioning of Hardware/Software	100%	On successful installation and Acceptance Sign-off from Bank
Hardware Appliance -AMC	Quarterly	AMC will be paid quarterly in arrears
FM Services (Bidder/OEM)	Quarterly	FMS Charges shall be paid quarterly in arrears

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

### **Fixed Price**

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

### **Taxes**

- 1) The consolidated fees and charges required to be paid by the Bank against each of the specified components under this RFP shall be all-inclusive amount with currently (prevailing) applicable taxes. The bidder shall provide the details of the taxes applicable in

the invoices raised on the Bank. Accordingly, the Bank shall deduct at source, all applicable taxes including TDS from the payments due/ payments to bidder. The applicable tax shall be paid by the bidder to the concerned authorities.

- 2) In case of any variation (upward or down ward) in Government levies / taxes / etc. up-to the date of providing services, the benefit or burden of the same shall be passed on or adjusted to the Bank. If the service provider makes any conditional or vague offers, without conforming to these guidelines, the Bank will treat the prices quoted as in conformity with these guidelines and proceed accordingly.
- 3) Goods and Services Taxes (GST) and its Compliance: -
  - i. Goods and Services Tax Law in India is a Comprehensive, multi-stage, destination-based tax that will be levied on every value addition. Bidder shall have to follow GST Law as per time being enforced along with certain mandatory feature mentioned hereunder.
  - ii. TDS (Tax Deducted on Source) is required to deduct as per applicable under GST Law on the payment made or credited to the supplier of taxable goods and services. It would enhance the tax base and would be compliance and self-maintaining tax law based on processes. The statutory compliances contained in the statutes include obtaining registration under the GST law by the existing assesses as well as new assesses, periodic payments of taxes and furnishing various statement return by all the registered taxable person.
  - iii. It is mandatory to pass on the benefit due to reduction in rate of tax or from input tax credit (ITR) to the Bank by way of commensurate reduction in the prices under the GST Law.
  - iv. If bidder as the case may be, is backlisted in the GST (Goods and Services Tax) portal or rating of a supplier falls below a mandatory level, as decided time to time may be relevant ground of cancellation of Contract.
- 4) Bank shall deduct tax at source, if any, as per the applicable law of the land time being enforced. The Service provider shall pay any other taxes separately or along with GST if any attributed by the Government Authorities including Municipal and Local bodies or any other authority authorized in this regard.

## 19 Service Level Agreement

Bidder shall ensure compliance with the SLAs defined in the RFP. This section describes the service levels that has been established for the services offered by the bidder to Bank. The bidder shall monitor and maintain the stated service levels to provide quality customer service to Bank.

S. N.	SERVICE AREA	EXPECTED SERVICE LEVEL	PENALTY
1.	SOFTWARE COMPONENT (ANY APPLICATION, OS ETC.) DOWN	PROBLEM SHOULD BE RESOLVED WITHIN 2 HOURS	NO PENALTY
2.	SOFTWARE COMPONENT (ANY APPLICATION, OS ETC.) DOWN	PROBLEM RESOLVED BETWEEN 2 HOURS TO 24 HOURS	2% OF MONTHLY PAYOUT

3.	SOFTWARE COMPONENT (ANY APPLICATION, OS ETC.) DOWN	PROBLEM RESOLVED AFTER 24 HOURS	5% OF MONTHLY PAYOUT
4.	BOTH DC AND DR SOFTWARE COMPONENT (ANY APPLICATION, OS ETC.) DOWN LEADINFG TO COMPLETE DISRUPTION		10% OF MONTHLY PAYOUT ON EACH OCCATION
5.	BOTH DC AND DR SOFTWARE COMPONENT (ANY APPLICATION, OS ETC.) DOWN LEADINFG TO COMPLETE DISRUPTION	DOWN BEYOND 24 HOURS	100% OF MONTHLY PAYOUT
6.	Audit of Patch Management Solution	Patch Management Solution infrastructure may be subjected to audit from Bank and/or third party. Audit observations to be closed as per Bank Policy in time frame. Vulnerability Analysis and Penetration Testing exercises conducted by Bank will also considered under this point.	Penalty of 2% for each week of delay in implementation of critical and important observations. Penalty of 2% for each repeated observations.
7.	Manpower services	Bidder to provide experienced and certified OEM manpower at Bank premises as per RFP. Any gap will attract penalty	After deducting pro rata charge for absence of resource, additional penalty of 500/- per absent resource per day will be deducted. In case bidder provides alternate adequately qualified resource for absent resource of OEM, no penalty shall be deducted. The penalty will be restricted up to 25% of monthly FM Charges.
8.	Incident response	All incidents must be categorized in 4 levels of	All incidents their root cause and action taken

		severity viz. Critical, High, Medium and Low (in decreasing order of severity). The severity rating of incidents will be defined in consultation with the selected Bidder by the Bank depending upon the business and compliance requirements. Closure of all incidences, once identified must be done as per the timelines given below: Critical events- within 4 hours High events- within 12 hours Medium and low events- within 24 hours	need to be logged and maintained incident register (hardcopy/ offline) to create a knowledgebase (softcopy/ online) for future reference.
--	--	--	---

### **19.1 Service Levels during implementation phase**

- 1) The Bidder is expected to complete the responsibilities that have been assigned as per the implementation timelines mentioned in Section - Project timelines.
- 2) Penalty would be levied for delivery, installation, and implementation delays for in-Scope components (such as product, ATS, Implementation, etc. part of this RFP) and shall be a maximum of 10% of the total cost of that solution from the finalized bidder for the Bank.

### **19.2 System Availability**

System availability is defined as  $\{( \text{Scheduled operation time} - \text{system downtime} ) / ( \text{scheduled operation time} )\} * 100\%$ .

Where:

- 1) Scheduled operation time means the scheduled operating hours of the System for the month. All planned downtime on the system would be deducted from the total operation time for the month to give the scheduled operation time.
- 2) System downtime subject to the SLA, means accumulated time during which the System is not available to the Bank's users or customers due to in-scope system or infrastructure failure, and measured from the time the Bank and / or its customers log a call with the Bidder's help desk of the failure or the failure is known to Bidder from the availability measurement tools to the time when the System is returned to proper operation.
- 3) Critical and Key infrastructure of Data Centre, Disaster Recovery Centre will be supported on 24x7X365 basis.
- 4) Downtime shall commence when the respective hardware and or it's associated software fails.
- 5) Uptime will be computed based on service availability of the in-scope components. Also, non-compliance with performance parameters for business and system / service degradation will be considered for downtime calculation.

- 6) Response may be telephonic or onsite. In case the issue cannot be resolved telephonically, Bidder (as per the criticality and nature of the issue) will provide onsite assistance at respective locations (DC, DRC) within response resolution window.
- 7) If any one or more of the components defined in —Critical at the Data Centre, Disaster Recovery Facility and are down resulting in non-availability of Solution, then affected services / components listed in the —Critical availability measurements table shall be considered for calculating the system downtime.
- 8) Service Levels will be complied with irrespective of the customizations that would undergo during the tenure of the Contract.
- 9) Typical Resolution time will be applicable if services are not available to the Bank's users and customers and there is a denial of agreed services.
- 10) The bidder to provide warranty &ATC support on all days (24X7X365) for period of contract
- 11) Bank has defined in-scope services and corresponding SLAs as under, Bank shall evaluate the performance of the Bidder on these SLAs compliance as per the periodicity defined.
- 12) The Successful Bidder shall provide, as part of monthly evaluation process, reports to verify the Successful Bidder's performance and compliance with the SLAs. Automated data capturing and reporting mechanism will be used for SLA reporting. The Bank will leverage existing/future EMS tools to monitor and manage the Solution/IT Infrastructure.
- 13) If the level of performance of Successful Bidder for a particular metric fails to meet the minimum service level for that metric, it will be considered as a Service Level Default.
- 14) Overall cap for penalties over the tenure of the contract will be 10% (ten percent) of the contract value.
- 15) Penalties if any, as defined by SLAs, shall be adjusted in the payment of a quarter. Balance penalties, if any shall be levied in the payment for the subsequent quarter.
- 16) The Bidder to provide Support contract backline to OEM for the complete duration of contract period. Letter to be provided by OEM for the backline proof, prior to release of payment.
- 17) Bidder agrees to ensure that all the items / products used for delivering services to the Bank including all components are new and are using state of the art technology. Bidder shall provide such proof of the new equipment (e.g. Copy of invoice etc.) to the Bank. In case of software supplied with the system, Successful Bidder shall ensure that the same is licensed and legally obtained in the name of end customer i.e., Bank with valid documentation made available to the Bank.

**Note:** All service level penalties will be reconciled at the end of every month.

### **19.3 Issue Criticality Classification**

- 1) The classification strategy has been envisaged to prioritize problem resolution based on Bank's priorities rather than in an ad-hoc manner. Classification framework will help Bank and the bidder to develop a shared understanding of the issue at hand, as well as the anticipated response and resolution timelines.
- 2) In order to improve the accuracy of the classification of an issue, application specific performance thresholds have been defined based on two characteristics, as mentioned below:
  - i. Impact: Number of users getting affected by the issue
  - ii. Availability: Uptime of the system, both, in absolute terms as well as percentage terms

Criticality Level	IT Infrastructure grouping	Response Times	Resolution Time
Critical	<ul style="list-style-type: none"> <li>System Software such as OS, Middleware, DB, etc. at DC</li> <li>Application Software at DC, for all the in-scope components</li> </ul>	10 Minutes	As per SLA
Key	<ul style="list-style-type: none"> <li>System Software such as OS, Middleware, DB, etc. at DRC</li> <li>Application Software at DRC, for all the in-scope components</li> </ul>	10 Minutes	As Per SLA
Individual	<ul style="list-style-type: none"> <li>System Software such as OS, Middleware, DB, etc. at DRC</li> <li>Application Software at DRC, for all the in-scope components</li> </ul>	10 Minutes	As Per SLA

- iii. In case of a disaster at DC or DR drill, DRC would be the primary site and then, infrastructure at DRC shall be considered as Critical and penalty shall be computed accordingly
- 3) If any hardware in High Availability (HA) mode fails while other is working with no impact on the availability of the underlying solution/application, in such a case, penalty shall be levied on the failed hardware. The failed hardware in HA mode should be replaced within 12 hours of the failure. If the bidder fails to meet the timeline, Bank shall levy a penalty at the rate of 1% of the product and services cost [Total Product & Service cost including Product cost (with 1/3 years warranty) + Implementation cost +AMC/ATS cost (for 2/4 Years)], for every 2 hours of delay thereof, on the failed hardware etc.
  - 4) If both the hardware components fail in HA mode, Bank shall levy penalty on the bidder for the service levels defaults, basis the service levels requirement mentioned here.
  - 5) For three (3) downtime occurrences within a stipulated time window of a calendar month, a sum equivalent to 1% of the product cost of the respective product would be levied as a penalty. This would be over and above the monthly service level default penalty.

#### **19.4 Service Level Default**

- 1) Service Levels will be measured on a monthly basis. The Bidder's performance to Service Levels will be assessed against Minimum Expected Service Level requirements for each criterion mentioned in the Availability measurement table.
- 2) An Availability Service Level Default will occur when, the Bidder fails to meet Minimum Service Levels, as measured on a monthly basis, for a particular Service Level.
- 3) Service Levels will include Availability measurements and Performance parameters.
- 4) Bidder will provide Availability Report on monthly basis and a review shall be conducted based on this report. A monthly report shall be provided to the Bank at the end of every month containing the summary of all incidents reported and associated Bidder performance measurement for that period.
- 5) Performance measurements would be accessed through reports, as appropriate to be provided by Bidder e.g. utilization reports, response time measurements reports, etc.
- 6) Cost Reference that is mentioned is billing value for the defaulted period & defaulted component for which SLA will be calculated.

7) Reports generated from EMS will be used for monitoring SLA

**8) Availability**

<b>Service Level Description</b>	<b>Minimum Service Level</b>	<b>Measurement Tools</b>	<b>Cost Reference for the contract period</b>
Availability of <b>Critical</b> Infrastructure	99.96%	Management System	Product cost at DC + Installation cost at DC + AMC & ATS cost at DC
Availability of <b>Key</b> infrastructure	99.3%	Management System	Product cost at DRC + Installation cost at DRC + AMC & ATS cost at DRC
Availability of <b>Key</b> infrastructure	99.3%	Management System	Product cost at location other than DC + Installation cost at the location + AMC & ATS cost at the location
Availability of <b>Individual components not impacting availability of the server/solution</b> infrastructure	96.7%	Management System	For every hour of delay thereof, penalty shall be levied at the rate of INR 5000

**9) Infrastructure Support**

- i. Response comprises acknowledgement of the problem and an initial analysis of the underlying cause
  - ii. Uptime – The amount of time that the system is available for normal use. (Do note that planned maintenance would also be classified as normal use.)
- 10) Bank expects the bidder to complete scope of the project including delivery and installation within the timeframe specified in this RFP. 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. The proposed rate of penalty would be 1 % of the value of the affected service or product per week of delay or non-compliance.
- 11) Delay in migration completion within stipulated timeline would invoke a penalty of INR 25,000 for every day of delay thereof.
- 12) Overall cap of all the penalties over the tenure of the contract will be 10% (ten percent) of the contract value.

**19.5 Performance Measurements**

Performance Measurements will be as follows:



Service Level Description	Measurement	Minimum Expected Service Level	Measurement Tools	Monthly Cost Allocation
Percentage of incidents for Critical components	Percentage of <b>incidents</b> completed within defined resolution criteria	100%	Management System	Total Product & Service cost, including Product cost (with 3 years warranty) + Implementation cost + ATS cost (for 2 years) at DC
Percentage of incidents for Key components	Percentage of <b>incidents</b> completed within defined resolution criteria	99%	Management System	Total Product & Service cost, including Product cost (with 3 years warranty) + Implementation cost + ATS cost (for 2 Years), at DRC
Software Service Requests	Percentage of Software <b>Service Requests</b> concluded (software installation, patches, bug fixes, errors) within defined timeframe/response-resolution window.	95%	Management System	Total cost, including license cost (with 3 years warranty) + Installation cost + ATS cost (for 2 Years), at DC and DRC
Incident Management	Percentage of incidents <b>escalated</b> according to the Incident Management matrix (as shown in Table 5 below)	99%	Management System	Total cost for relevant product, including license cost (with 3 years warranty) + Installation cost + ATS cost (for 2 Years), at DC and DRC, whichever, is applicable
Down time for servicing	Each planned down - time for system servicing (up gradation, bug fixing, patch uploads, regular maintenance etc.) will not be more than 4 hours.	98%	Management System	For downtime over and above the scheduled / permissible window, penalty of INR 5000 for every 30 minutes of delay above 1 hour of scheduled downtime

Service Level Description	Measurement	Minimum Expected Service Level	Measurement Tools	Monthly Allocation Cost
	<p>This activity will not be carried out during business hours.</p> <p>However, such activities which require more than 1 hour or required to be carried out during business hours, will be scheduled in consultation with Bank. In case, downtime exceeds the planned hours, the additional time taken for servicing will be considered for infrastructure or system downtime as per availability measurements table.</p>			
Modification (Customization/ Enhancements) resolution for Application software	Bidder to ensure that all modifications, enhancements reported by the BANK will be duly sized, mutually agreed with the BANK and resolved as per the defined timeframes	96%	Management Solution	Monthly ATS of the affected services

### **19.6 Penalty Computation**

- 1) In the event of Service Level Default, bidder shall pay Bank a penalty that will be computed in accordance with the following formula:
  - i.  $\text{Monthly Service Level Default} = \text{Minimum Service Level (for a month)} - \text{Actual Service Level (for a month)}$
- 2) Total amount of penalty, bidder is obligated to pay Bank, shall be reflected on the invoice provided to Bank in the quarter, after the quarter in which the Service Levels were assessed. Bank shall be entitled to deduct the penalty amount from the amounts payable by Bank to the selected bidder as per the invoice.
- 3) **Example**

Scenario	Result
----------	--------

<p>The achieved availability of Server Infrastructure has been measured to be 98% in a particular assessment month.</p>	<p>For this example, let's assume, monthly Availability Service level is of 99.95%; for availability of 98%, penalty invoked would be of 1.95% of total cost of products and services of the failed component.</p> <p><u>Cost Reference for 5-year tenure</u></p> <p>Server equipment cost = INR 1 crores (approximately)</p> <p>Server equipment AMC cost = INR 30,00,000 (approximately)</p> <p>Total cost of product and services for a Server equipment = 1,30,00,000</p> <p>As mentioned above, for Availability Service level default of more than 99.5% and less than 98%, a penalty of 2% would be levied of the total cost of products and services calculated above.</p> <p>Thus, 2% of 1, 30,00,000 i.e. INR 2,60,000.</p>
---	---

### 19.7 Availability Service Credit Computation

- 1) In the event of an Availability Service Level Default, the Bidder shall pay the Bank an Availability Service Credit that will be computed in accordance with the following formula:
  - i. Monthly Service Level Default = Minimum Service Level – Monthly Actual Service Level
  - ii. Availability Service Credit = Quarterly Service level default X (Summation of Cost References)
- 2) In the event that an Availability Service Level Default has occurred for more than one service level requirement, the sum of the corresponding Availability Service Credits shall be credited to the Bank. Bidder shall review with the Bank, on a monthly basis from the start of Contract Execution, any entitlement of the Bank to an Availability Service Credit.
- 3) The total amount of Availability Service Credit that Bidder is obligated to pay the Bank shall be reflected on the invoice provided to the Bank in the quarter after the quarter in which the Service Levels were assessed. The Bank shall be entitled to deduct the Availability Service Credit amount from the amounts payable by the Bank to the Bidder as per the invoice.

#### **Example 1**

Assume for a particular service level requirement (eg: Availability of Key Business Infrastructure Elements), the minimum service level is 99.5% During a Service Assessment period; the service level achieved is 96.5%:

The Product licenses Cost and its associated Software Cost ~ Rs.2 crores

Annual Technical Support Cost ~ Rs.5 crores

Total Cost of Product and Services billing value for the defaulted period & defaulted deliverable ~ Rs.7 crores

The Availability Service Credit due to the Bank would be computed as follows:

Minimum Service Level

Monthly Service Level Default =  $M1 = 99.5 - 96.5 = 3$

Availability Service Credit for  $M1 = 3\% * (2 \text{ crores} + 5 \text{ crores}) = \text{Rs.}21,00,000$

Bidder has to note that the total cost of products and services is inclusive of taxes for the purpose of computation of the service level and service credit.

### **19.8 Tables of Incident Matrix**

<b>Time within which Incident is to be reported (if unresolved)</b>	<b>Escalation Hierarchy</b>
15 min	Senior Manager-IT of the BANK
1 hour	Chief Manager -IT
2 hours	Assistant General Manager (IT) / Deputy General Manager (IT)
> 4 hours	General Manager (IT)

## **20 Reporting of Material Adverse Events and Incident Management**

The Bidder shall promptly report any material adverse events, including but not limited to data breaches, denial of service attacks, service unavailability, security vulnerabilities, unauthorized access, system failures, or any other incidents that may impact the Bank's operations or data integrity. Such incidents shall be reported to the Bank immediately upon identification, enabling the Bank to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines. The service provider shall provide all relevant details and updates regarding the incident, including the nature, scope, impact, and corrective actions taken, in accordance with the Bank's incident reporting procedures.

## **21 Insurance**

The equipment (hardware/software, etc.) supplied under the contract shall be fully insured by the Service Provider against loss or damage incidental to manufacture or acquisition, transportation, storage, delivery, and installation. The insurance shall be obtained by the Service Provider, naming Central Bank of India as the beneficiary, for an amount equal to 100% of the invoiced value of the goods on an "all risks" basis, covering risks such as damage, theft, fire, or natural disasters. The period of insurance shall remain in effect until the supplied components are accepted by the Bank, and the rights to the property are transferred to the Bank at its premises. In the event of any loss

or damage, the Service Provider shall initiate and pursue the claim until settlement. Additionally, the Service Provider must promptly make arrangements for the repair and/or replacement of any damaged items, irrespective of the settlement of the claim by the underwriters. Furthermore, the Service Provider shall ensure that the insurance policy remains valid throughout the supply, transportation, and installation period, and any gaps in coverage shall be rectified immediately. The Service Provider shall also provide the Bank with necessary documentation of the insurance policy, claim details, and any associated correspondence with the underwriters.

## **22 Order Cancellation**

Bank reserves the right to cancel the contract placed on the service provider and recover expenditure incurred by the Bank under the following circumstances. If the service provider commits a breach of any of the terms and conditions of the bid, or if the service provider goes into liquidation, voluntarily or otherwise, the Bank reserves the right to cancel the contract. Additionally, if an attachment is levied or continues to be levied for a period of seven days upon the effects of the bid, the Bank may take appropriate action. If the service provider fails to complete the assignment as per the timelines prescribed in the RFP and any extension allowed, it will be considered a breach of contract, and the Bank reserves its right to cancel the order in the event of delay and forfeit the bid security/performance Bank guarantee as liquidated damages for the delay. If deductions on account of liquidated damages exceed more than 10% of the total contract price, the Bank reserves the right to cancel the contract.

After the award of the contract, if the service provider does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one month's notice for the same. In this event, the service provider is bound to make good the additional expenditure that the Bank may have to incur in executing the balance contract. This clause is applicable if, for any reason, the contract is cancelled. The Bank reserves the right to recover any dues payable by the service provider from any amount outstanding to the credit of the service provider, including pending bills and/or invoking the Bank guarantee under this contract.

In addition to the cancellation of the purchase order, the Bank reserves the right to appropriate the damages from the Bid Security / Performance Bank Guarantee given by the service provider and/or foreclose the Bank guarantee given by the service provider against the advance payment and may take appropriate action. Further, in case of failure to adhere to the terms and conditions of the RFP in totality, concealment of facts in the tender documents, or failure to fulfill the contractual obligations of the Purchase order, the Bank may debar/blacklist the service provider from participating in future tender processes. The Bank reserves the right to inform IBA/other Banks about blacklisting the service provider in case of default in service or delay leading to financial or reputational loss, loss of time of the Bank.

## **23 Indemnity**

- 1) The Bidder shall indemnify the Bank, and shall always keep indemnified and hold the Bank, its employees, personnel, officers, directors, harmless from and against any and all losses, liabilities, claims, actions, costs and expenses (including attorney's fees) relating to, resulting directly or indirectly from or in any way arising out of any claim, suit or proceeding brought against the Bank as a result of:
  - i. Bank's authorized / bonafide use of the Deliverables and/or the Services provided by Bidder under this RFP or any or all terms and conditions stipulated in the SLA (Service level Agreement) or PO and/or
  - ii. Relating to or resulting directly from infringement of any third party patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project.
  - iii. An act or omission of the Bidder, employees, agents, sub-contractors in the performance of the obligations of the Bidder under this RFP or, any or all terms and conditions stipulated in the SLA(Service level Agreement) or Purchase Order(PO) and/or
  - iv. Claims made by employees or subcontractors or subcontractors' employees, who are deployed by the Bidder, against the Bank and/or
  - v. Breach of any of the term of this RFP or breach of any representation or false representation or inaccurate statement or assurance or covenant or warranty of the Bidder under this RFP or; any or all terms and conditions stipulated in the SLA (Service level Agreement) or PO and/or
  - vi. Any or all Deliverables or Services infringing any patent, trademarks, copyrights or such other Intellectual Property Rights and/or
  - vii. Breach of confidentiality obligations of the Bidder contained in this RFP or; any or all terms and conditions stipulated in the SLA (Service level Agreement) or PO and/or
  - viii. Negligence or gross misconduct attributable to the Bidder or its employees, agent or sub-contractors.
- 2) The Bidder shall further indemnify the Bank against any loss or damage arising out of claims of infringement of third-party copyright, patents, or other intellectual property issued or registered in India, provided however,
  - i. The Bank notifies the Bidder in writing immediately on aware of such claim,
  - ii. The Bidder has sole control of defense and all related settlement negotiations,

- iii. The Bank provides the Bidder with the assistance, information and authority reasonably necessary to perform the above, and
  - iv. The Bank does not make any statement or comments or representations about the claim without prior written consent of the Bidder, except under due process of law or order of the court. It is clarified that the Bidder shall in no event enter into a settlement, compromise or make any statement (including failure to take appropriate steps) that may be detrimental to the Bank's (and/or its customers, users and Bidders) rights, interest and reputation.
- 3) The Bidder shall compensate the Bank for direct financial loss suffered by the Bank, if the Bidder fails to fix bugs, provide the Modifications / Enhancements / Customization as required by the Bank as per the terms and conditions of this RFP and to meet the Service Levels as per satisfaction of the Bank.
- 4) Additionally, the Bidder shall indemnify, protect and save the Bank against all claims, losses, costs, damages, expenses, action, suits and other proceedings, suffered by Bank due to the following reasons:
- i. that the Deliverables and Services delivered or provided under this Agreement infringe a patent, utility model, industrial design, copyright, trade secret, mask work or trademark in any country where the Deliverables and Services are used, sold or received; and/or The Bidder shall indemnify the Bank in case of any mismatch of ITC (Input Tax Credit) in the GSTR 2A, where the Bank does not opt for retention of GST component on supplies.
  - ii. all claims, losses, costs, damages, expenses, action, suits and other proceedings resulting from infringement of any patent, trade-marks, copyrights etc. or such other statutory infringements under any laws including the Copyright Act, 1957 or Information Technology Act, 2000 or any Law, rules, regulation, bylaws, notification time being enforced in respect of all the Hardware, Software and network equipment or other systems supplied by them to the Bank from whatsoever source, provided the Bank notifies the Bidder in writing as soon as practicable when the Bank becomes aware of the claim however:
    - The Bidder has sole control of the defense and all related settlement negotiations.
    - The Bank provides the Bidder with the assistance, information and authority reasonably necessary to perform the above and bidder is aware of the rights to make any statements or comments or representations about the claim by Bank or any regulatory authority. Indemnity would be limited to court or arbitration awarded damages and shall exclude indirect and incidental damages and compensations.

- 5) Bidder shall have no obligations with respect to any Infringement Claims to the extent that the Infringement Claim arises or results from:
- i. Bidder's compliance with Bank's specific technical designs or instructions (except where Bidder knew or should have known that such compliance was likely to result in an Infringement Claim and Bidder did not inform Bank of the same);
  - ii. Inclusion in a Deliverable of any content or other materials provided by Bank and the infringement relates to or arises from such Bank materials or provided material;
  - iii. Modification of a Deliverable after delivery by Bidder to Bank if such modification was not made by or on behalf of the Bidder;
  - iv. operation or use of some or all of the Deliverable in combination with products, information, specification, instructions, data, materials not provided by Bidder; or (v) use of the Deliverables for any purposes for which the same have not been designed or developed or other than in accordance with any applicable specifications or documentation provided under the applicable Statement of Work by the Bidder; or
  - v. Use of a superseded release of some or all of the Deliverables or Bank's failure to use any modification of the Deliverable furnished under this Agreement including, but not limited to, corrections, fixes, or enhancements made available by the Bidder.
- 6) In the event that Bank is enjoined or otherwise prohibited, or is reasonably likely to be enjoined or otherwise prohibited, from using any Deliverable as a result of or in connection with any claim for which Bidder is required to indemnify Bank under this section according to a final decision of the courts or in the view of Bidder, Bidder, may at its own expense and option:
- (i) Procure for Bank the right to continue using such Deliverable;
  - (ii) Modify the Deliverable so that it becomes non-infringing without materially altering its capacity or performance;
  - (iii) Replace the Deliverable with work product that is equal in capacity and performance but is non-infringing; or (iv) If such measures do not achieve the desired result and if the infringement is established by a final decision of the courts or a judicial or extrajudicial settlement, the Bidder shall refund the Bank the fees effectively paid for that Deliverable by the Bank subject to depreciation for the period of Use, on a straight line depreciation over a 5 year period basis. The foregoing provides for the entire liability of the Bidder and the exclusive remedy of the Bank in matters related to infringement of third party intellectual property rights.
- 7) The Bank warrants that all software, information, data, materials and other assistance provided by it under this Agreement shall not infringe any intellectual property rights of third parties, and agrees that it shall at all times indemnify and hold Bidder harmless from any loss, claim, damages, costs, expenses, including Attorney's fees, which may be incurred as a result of any action or claim that may be made or initiated against it by any third parties alleging infringement of their rights.



## **24 Confidentiality & Non-Disclosure**

- 1) The bidder is bound by this agreement for not disclosing the Banks data and other information. Resources working in the premises of the Bank are liable to follow the rules and regulations of the Bank.
- 2) The document contains information confidential and proprietary to the Bank. Additionally, the bidder will be exposed by virtue of the contracted activities to the internal business and operational information of the Bank, affiliates, and/or business partners, disclosure of receipt of this tender or any part of the aforementioned information to parties not directly involved in providing the requested services could result in the disqualification of the bidders, premature termination of the contract, or legal action against the bidder for breach of trust.
- 3) No news release, public announcement or any other reference to the order, relating to the contracted work if allotted with the assignment or any program hereunder shall be made without written consent from the Bank.
- 4) As the bidder providing support services for multiple Banks, the bidder at all times should take care to build strong safeguards so that there is no mixing together of information/ documents, records and assets is happening by any chance.
- 5) The bidder should undertake to maintain confidentiality of the Banks information even after the termination / expiry of the contracts.
- 6) The Non-Disclosure Agreement (NDA) should be entered in to between the Bank and the successful bidder within a period of 21 days from, the date of acceptance of purchase order.

### Guarantee on Software License

The bidder shall guarantee that the software supplied under this contract to the Bank is licensed and legally obtained. Software supplied should not have any embedded malicious and virus programs. Bidder must comply RBI circular on “Cyber Security Framework for Banks” and assurance from the respective OEMs/Application providers that the application is free from embedded malicious/fraudulent code

## **25 Force Majeure**

- 1) The parties shall not be liable for default or non-performance of the obligations under the contract, if such default or non-performance of the obligations under this contract is caused by any reason or circumstances or occurrences beyond the control of the parties, as a result of force majeure. For the purpose of this clause, “Force Majeure” shall mean an event beyond the control of the parties, including but not limited to, due to or as a result of or caused by acts of God, wars, epidemic/pandemic, insurrections, riots, earth quake and fire, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation.
- 2) In the event of any such intervening Force Majeure, each party shall notify the other party in writing of such circumstances and the cause thereof immediately within seven business days. Unless otherwise directed by the other party, the party pleading Force Majeure shall continue to perform/render/discharge other obligations as far as they can reasonably be attended/fulfilled and shall seek all reasonable alternative means for performance affected by the Event of Force Majeure.

- 3) In such a case, the time for performance shall be extended by a period(s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months due to force majeure situation, the parties shall hold consultations with each other in an endeavour to find a solution to the problem. However bidder shall be entitled to receive payments for all services actually rendered up to the date of termination of date of agreement. The financial constraints by way of increased cost to perform the obligations shall not be treated as a force majeure situation if the obligations can otherwise be performed.

## **26 Resolution of Disputes**

- 1) The Bank and the bidder shall make every effort to resolve amicably, by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the contract. If after thirty days from the commencement of such informal negotiations, the Bank and the Bidder have been unable to resolve amicably a contract dispute, either party may require that the dispute be referred for resolution by formal arbitration.
- 2) All questions, disputes or differences arising under and out of, or in connection with the contract shall be referred to a sole arbitrator to be appointed mutually by the parties and in case of failure to appoint a sole arbitrator within 15 days from the raising of dispute the same shall be referred to the Arbitration Tribunal: one Arbitrator to be nominated by the Bank and the other to be nominated by the Bidder and the Presiding Arbitrator shall be appointed by the two Arbitrators appointed by the parties.
- 3) The decision of the Arbitration Tribunal shall be final and binding on the parties. The Arbitration and Reconciliation Act 1996 shall apply to the arbitration proceedings and the venue of the arbitration shall be Mumbai. The Language of Arbitration will be English. Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, bidder will continue to perform its contractual obligations and the Bank will continue to pay for all products and services that are accepted by it, provided that all products and services are serving as per the agreed scope between the parties.
- 4) If a notice has to be sent to either of the parties following the signing of the contract, it has to be in writing and shall be first transmitted by facsimile transmission, by postage prepaid registered post with acknowledgement due or by a reputed courier service, in the manner as elected by the Party giving such notice. All notices shall be deemed to have been validly given on (i) the business date immediately after the date of transmission with confirmed answer back, if transmitted by facsimile transmission, or (ii) on the date of acknowledgment signed by the receiver or (iii) the business date of receipt, if sent by courier.
- 5) This RFP shall be governed and construed in accordance with the laws of India. The courts of Mumbai alone and no other courts shall be entitled to entertain and try any dispute or matter relating to or arising out of this RFP.

## **27 Format of the Letter of undertaking of Authenticity to be submitted by the Bidder.**

The successful bidder has to submit the letter of undertaking of Authenticity and Undertaking at the time of acceptance of the letter of intent. The undertaking from OEMs needs to be provided to the Bank for the activities owned by them in coordination with the bidder as per

the details mentioned in the document along with the pricing. The format for the same is as below.

“We undertake that all the components/parts/software used in the supplied devices shall be original, new components/ parts/ software only, from respective OEM/OSDs of the products and that no refurbished/ duplicate/ second hand components/ parts/ software are being used or shall be used.

We also undertake that in respect of licensed operating system, if asked for by you in the Purchase Order, the same shall be supplied along with the authorized license certificate and also that it shall be sourced from the authorized source.

We hereby undertake to produce the certificate from our OEM/OSD supplier in support of above undertaking at the time of implementation. It will be our responsibility to produce such letters from our OEM/OSD suppliers at the time of release of PO or within a reasonable time. In case of default and we are unable to comply with the above at the time of delivery or during installation, for the software items already billed, we agree to take back the software/items without demur, if already supplied and return the money, if any paid to us by you in this regard”.

## **28 Sub-Contractor/ Independent Contractor**

Nothing herein contained will be construed to imply a joint venture, partnership, principal agent relationship or co-employment or joint employment between the Bank and Bidder. Bidder, in furnishing services to the Bank hereunder, is acting only as an independent contractor. Bidder does not undertake by this Agreement or otherwise to perform any obligation of the Bank, whether regulatory or contractual, or to assume any responsibility for the Bank’s business or operations. The parties agree that, to the fullest extent permitted by applicable law; Bidder has not, and is not, assuming any duty or obligation that the Bank may owe to its customers or any other person. The bidder shall follow all the rules, regulations statutes and local laws and shall not commit breach of any such applicable laws, regulations etc. In respect of sub-contracts, as applicable – If required by the Bidders, should provide complete details of any subcontractor/s used for the purpose of this engagement. It is clarified that notwithstanding the use of sub-contractors by the Bidder, the Bidder shall be solely responsible for performance of all obligations under the SLA/NDA (Non-Disclosure Agreement) irrespective of the failure or inability of the subcontractor chosen by the Bidder to perform its obligations. The Bidder shall also have the responsibility for payment of all dues and contributions, as applicable, towards statutory benefits including labour laws for its employees and sub-contractors or as the case may be. Bidder should take Bank’s prior written permission before subcontracting/ resource outsourcing of any work related to the performance of this RFP or as the case may be, which permission shall not be unreasonably withheld by the Bank. The bidder should ensure that the due diligence and verification of antecedents of employees/personnel deployed by him for this project are completed and is available for scrutiny by the Bank.

## **29 Assignment**

Bank may assign the Project and the solution and services provided therein by Bidder in whole or as part of a corporate reorganization, consolidation, merger, or sale of substantially all of its assets. The Bank shall have the right to assign such portion of the facilities management services to any of the Contractor/sub-contractor, at its sole option, upon the occurrence of the

following: (i) Bidder refuses to perform; (ii) Bidder is unable to perform; (iii) termination of the contract with Bidder for any reason whatsoever; (iv) expiry of the contract. Such right shall be without prejudice to the rights and remedies, which the Bank may have against Bidder. Bidder shall ensure that the said sub-contractors shall agree to provide such services to the Bank at no less favourable terms than that provided by Bidder and shall include appropriate wordings to this effect in the agreement entered into by Bidder with such sub-contractors. The assignment envisaged in this scenario is only in certain extreme events such as refusal or inability of Bidder to perform or termination/expiry of the contract/project.

### **30 Execution of Contract, SLA & NDA**

The bidder and Bank should execute:

- 1) Contract, which would include all the services and terms and conditions of the services to be extended as detailed herein and as may be prescribed by the Bank and
- 2) Non-disclosure Agreement.
- 3) The bidder should execute the contract, SLA and NDA within 21 days from the date of acceptance of the Purchase Order. In case of any discrepancy among the RFP, SLA and Purchase Order, the RFP clauses shall prevail.

### **31 Bidder's Liability**

The Bidders aggregate liability in connection with obligations undertaken as a part of the project regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actuals and limited to the value of the contract. The Bidders liability in case of claims against the Bank resulting from misconduct or gross negligence of the Bidder, its employees and subcontractors or from infringement of patents, trademarks, copyrights(if any) or breach of confidentiality obligations shall be unlimited. In no event shall the Bank be liable for any indirect, incidental or consequential damages or liability, under or in connection with or arising out of this tender and subsequent agreement or services provided. The bidder should ensure that the due diligence and verification of antecedents of employees/personnel deployed by him for execution of this contract are completed and is available for scrutiny by the Bank.

### **32 Information Ownership**

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

security safeguards or part of it shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any Bank location.

### **33 Inspection, Audit, Review, Monitoring & Visitations**

All OEM/Bidder records with respect to any matters / issues covered under the scope of this RFP/project shall be made available to the Bank at any time during normal business hours, not more than 2 audits per year, to audit, examine, and make excerpts or transcripts of all relevant data. Such records are subject to examination. The cost of such audit will be borne by the Bank. Bidder shall permit audit by internal/external auditors of the Bank or RBI to assess the adequacy of risk management practices adopted in overseeing and managing the outsourced activity/arrangement made by the Bank. Bank shall undertake a periodic review of service provider/BIDDER outsourced process to identify new outsourcing risks as they arise. The BIDDER shall be subject to risk management and security and privacy policies that meet the Bank's standard. In case the BIDDER outsourced to third party, there must be proper Agreement / purchase order with concerned third party. The Bank shall have right to intervene with appropriate measure to meet the Bank's legal and regulatory obligations. Access to books and records/Audit and Inspection would include:-

- 1) Ensure that the Bank has the ability to access all books, records and information relevant to the outsourced activity available with the BIDDER. For technology outsourcing, requisite audit trails and logs for administrative activities should be retained and accessible to the Bank based on approved request.
- 2) Provide the Bank with right to conduct audits on the BIDDER whether by its internal or external auditors, or by external specialist appointed to act on its behalf and to obtain copies of any audit or review reports and finding made on the service provider in conjunction with the services performed for the Bank.
- 3) Include clause to allow the reserve Bank of India or persons authorized by it to access the Bank's documents: records of transactions, and other necessary information given to you, stored or processed by the BIDDER within a reasonable time. This includes information maintained in paper and electronic formats.
- 4) Recognized the right of the reserve Bank to cause an inspection to be made of a service provider of the Bank and its books and account by one or more of its officers or employees or other persons. Banks shall at least on an annual basis, review the financial and operational condition of the BIDDER. Bank shall also periodically commission independent audit and expert assessment on the security and controlled environment of the BIDDER. Such assessment and reports on the BIDDER may be performed and prepared by Bank's internal or external auditors, or by agents appointed by the Bank.
- 5) Any such audit shall be conducted expeditiously, efficiently, and at reasonable business hours after giving due notice to the Bidder which shall not be less than 10 days. The Bank shall not have access to the proprietary data of, or relating to, any other customer of Bidder, or a third party or Bidder's cost, profit, discount and pricing data. The audit shall not be permitted if it interferes with Bidder's ability to perform the services in accordance with the service levels, unless the Bank relieves Bidder from meeting the applicable service levels. The audit shall not be performed by any competitor of the Bidder. The auditor including regulatory auditor shall sign the confidentiality undertaking with the Bidder before conducting such audit.

### **34 Monitoring**

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

### **35 Visitations**

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

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

### **36 Information Security**

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

### **37 Intellectual Property Rights**

The Bidder claims and represents that it has obtained appropriate rights to provide the Deliverables upon the terms and conditions contained in this RFP. The Bank agrees and acknowledges that same as expressly provided in this RFP, all Intellectual Property Rights in relation to the Hardware, Software and Documentation and any adaptations, translations and derivative works thereof whether protectable as a copyright, trade mark, patent, trade secret design or otherwise, provided by the Bidder during, in connection with or in relation to fulfilling its obligations under this RFP belong to and shall remain a property of the Bidder or its licensor. During the Term of this Project and, if applicable, during the Reverse Transition Period, Bank grants Bidder a right to use at no cost or charge the Hardware and Software licensed to the Bank, solely for the purpose of providing the Services.

The Bidder shall be responsible for obtaining all necessary authorizations and consents from third party licensors of Hardware and Software used by Bidder in performing its obligations under this Project. If a third party's claim endangers or disrupts the Bank's use of the Hardware and Software, the Bidder shall at no further expense, charge, fees or costs to the Bank,

- Obtain a license so that the Bank may continue use of the Software in accordance with the terms of this tender and subsequent Agreement and the license agreement; or

- Modify the Software without affecting the functionality of the Software in any manner so as to avoid the infringement; or
- Replace the Software with a compatible, functionally equivalent and non-infringing product. All third party Hardware/software / service/s provided by the bidder in the scope of the RFP will be the responsibility of the bidder if any discrepancy or infringement is encountered. The Bank shall not be held liable for and is absolved of any responsibility or claim/Litigation or penal liability arising out of the use of any third party software or modules supplied by the Bidder as part of this Project.

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

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

relieve either party of its confidentiality obligations with respect to the proprietary and confidential information or material of the other party

### **38 Termination**

#### **38.1 Termination for Default**

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

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

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

Bidder shall also have the right to terminate the agreement if the Bank commits a breach of the terms and conditions of the agreement and, where such breach is curable, fails to cure the same within 15 days provided for curing such breach.

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

#### **38.2 Termination for Insolvency**

If either party becomes Bankrupt or insolvent, has a receiving order issued against it, with its creditors, or, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if either party takes or suffers any other analogous action in consequence of debt; then other party plans to, at any time, terminate the contract by giving written notice of 60 days to the party becoming Bankrupt etc. If the contract is terminated by either party in terms of this Clause, Bank shall be liable to make payment of the entire amount due under the contract for which services have been rendered by the Selected Bidder.

#### **38.3 Termination- Key Terms & Conditions**

Either Party reserves the right to terminate the agreement with the other party at any time by giving 30 (thirty) days prior written notice to the other party.



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

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

#### **38.4 Right to Transfer IT Outsourcing Arrangements**

In the event of termination, the Bank reserves the right to orderly transfer the proposed IT outsourcing arrangement to another service provider, if necessary or desirable, to ensure minimal disruption of services. This transfer shall be managed in an efficient manner, with the bidder cooperating fully with the Bank to facilitate this process, including transferring knowledge, data, and providing assistance as required.

#### **38.5 Exit Option & Contract Re-Negotiation**

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

- 1) Failure of the successful bidder to accept the contract and furnish the Performance Guarantee within 21 days of receipt of purchase contract.
- 2) Substantial delay in delivery, performance or implementation of the solution beyond the specified period.
- 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)

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

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

### **39 Privacy & Security Safeguards**

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

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

- 2) The Bidder hereby agrees and confirms that they will disclose, forthwith, instances of security breaches.
- 3) The Bidder hereby agrees that they will preserve the documents.
- 4) The Bidder shall provide to the Bank, the details of all data related to the Bank and its customers that the service Provider captures, Processes and stores.
- 5) The Bidder may only share customer data with third parties when legally required, with prior consent, or for necessary operational purposes, ensuring compliance with confidentiality and data protection agreements.

#### **40 Governing Law and Jurisdiction**

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

#### **Statutory and Regulatory Requirements**

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

#### **41 Compliance**

- 1) The Service Provider (SP) agrees to comply with all applicable laws, regulations, and industry standards, including but not limited to the **Information Technology Act, 2000, Digital Personal Data Protection Act, 2023, RBI's "Master Direction on Outsourcing of Information Technology Services** and any other relevant data protection or privacy laws. The SP shall ensure that the products and services provided under this agreement comply with all regulatory requirements, including guidelines set by authorities such as the **Reserve Bank of India (RBI)** and **FEMA**.

The clauses under RBI master Directives on Outsourcing of IT Services are:-

- i. **Effective access by Bank to all record:** Bank should have effective access to all data, books, records, information, logs, alerts and business premises relevant to the outsourced activity, available with the Vendor.

- ii. **Vendor to Provide Details of Data:** The Vendor to provide to Bank the details of data (related to Bank and its customers) captured, processed and stored.
  - iii. **Data / Information which can be shared:** Vendor is not permitted to share any type of data/information with Bank's customer and / or any other party.
  - iv. **Information of Third Parties :** Bank will have right to seek information from the Vendor about the third parties (in the supply chain) engaged by the former;
  - v. **Prior Approval / Consent of Bank for use of Sub- contractors :** Vendor to take prior approval/ consent of the Bank for use of sub-contractors for all or part of an outsourced activity.
  - vi. **Skilled Resources of Vendor for Core Services :** Vendor to have provision to consider its skilled resources who provide core services as "essential personnel" so that a limited number of staff with back-up arrangements necessary to operate critical functions can work on-site during exigencies (including pandemic situations).
  - vii. **Back to Back Arrangements between Vendor and OEM:** There should be suitable back-to-back arrangements between Vendor and the OEMs, if any.
  - viii. **No relationship of master and servant or employer and employee:** Notwithstanding what is stated elsewhere in this agreement, this agreement does not create any relationship of Master and servant or Employer and employee as between the Bank on the one hand and the Vendor and/or the personnel employed/engaged by the Vendor on the other hand. The parties expressly understand and agree that this agreement broadly covers in respect of specific job/s to be performed by the Service Provider.
- 2) The SP shall adhere to the Bank's **Information Security Policy** and implement necessary controls for system security, including access control, data protection, and encryption, at all levels (e.g., database, operating system, application). The SP must also ensure the hardening of systems to protect against vulnerabilities.

#### **41.1 Adherence to Cyber Security Policy**

- 1) Vendors are responsible for complying with the security standards or desired security aspects of all the ICT resources in line with regulatory guidelines from time to time as well as Bank's IT/Information Security / Cyber Security Policy guidelines. Such guidelines will be shared with Vendor.
- 2) Vendor should ensure Data Security and protection of facilities/application managed by them. The deputed persons should be aware about Bank's IT/IS/Cyber security policy guidelines and have to maintain the utmost secrecy & confidentiality of the Bank's data including process performed. At any time, if it comes to the notice of the Bank that data has been compromised/disclosed/misused/misappropriated then Bank would take suitable action as deemed fit and selected vendor would be required to fully compensate the Bank of loss incurred by the Bank.

- 3) Vendor has to agree and provide undertaking not to disclose any Bank information and will maintain confidentiality of Bank information as per policy of the Bank and will sign “Non-Disclosure Agreement” document provided by Bank.
- 4) The Service provider shall put in place necessary controls within its organization for maintaining confidentiality of the Bank’s and its customer’s data.

#### **41.2 Compliance with Laws**

- 1) Compliance with all applicable laws: Successful bidder shall undertake to observe, adhere to, abide by, comply with the Bank about all laws in force or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this scope of work.
- 2) Compliance in obtaining approvals/permissions/licenses: Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project.

#### **42 Violation of Terms**

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

#### **43 Corrupt & Fraudulent Practices**

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

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

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

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

#### **44 Publicity**

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

#### **45 Entire Agreement; Amendments**

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

#### **46 Survival and Severability**

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

#### **47 Bidding Document**

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

##### **47.1 Amendments to Bidding Documents**

At any time prior to the last Date and Time for submission of bids, the Bank may, for any reason, modify the Bidding Document by amendments at the sole discretion of the Bank. All amendments will be either uploaded in the website or shall be delivered by hand / post / courier or through e-mail or faxed to all prospective bidders, who have received the bidding document and will be binding on them. For this purpose bidders must provide name of the contact person, mailing address, telephone number and FAX numbers on the covering letter sent along with the bids.

In order to provide, prospective bidders, reasonable time to take the amendment if any, into account in preparing their bid, the Bank may, at its discretion, extend the deadline for submission of bids.

##### **47.2 Period of Validity**

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

##### **47.3 Last Date and Time for Submission of Bids**

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

#### **47.4 Late Bids**

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

#### **47.5 Modifications and/or Withdrawal of Bids**

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

#### **47.6 Clarification of Bids**

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

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

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

### **48 Signing of Contract**

The successful bidder(s) to be called as bidder, shall be required to enter into an Agreement with the Bank, within 21 days of the award of the work order (when provided) or within such extended period as may be specified by the Bank.

### **49 Sustainable Sourcing**

The Supplier shall adhere to Sustainable Sourcing practices including but not limited to the use of environment friendly materials, ethical labor practices and compliance with relevant local and international regulations. The Supplier shall provide documentation or certifications demonstrating their commitment to Sustainable Sourcing upon request. Failure to comply with these requirements may result in contract termination.

### **50 Remote Access:**

Any type of remote access will not be allowed outside Bank's Network.

### **51 Business Continuity and Disaster Recovery**

#### **51.1 Business Continuity Plan (BCP)**

The Service Provider shall have a documented Business Continuity Plan in place, which outlines the strategies for maintaining service availability in the event of an unexpected incident. The BCP should include, but is not limited to:

- 1) Detailed procedures for mitigating and recovering from various business disruptions.
- 2) Identification of key personnel, roles, and responsibilities in a crisis.

- 3) Communication plans to inform both the Service Provider and Customer of significant disruptions and progress towards recovery.

## **51.2 Disaster Recovery Plan (DRP)**

The Service Provider shall maintain a Disaster Recovery Plan to restore critical services and infrastructure in the event of a disaster, including:

- 1) Specific recovery objectives, such as Recovery Time Objective (RTO) and Recovery Point Objective (RPO), to be met for each service.
- 2) Procedures for data backup, storage, and retrieval.
- 3) Clear steps to restore services to full functionality, including resource allocation and escalation procedures.

## **52 Obligation to Cooperate with relevant authorities in case of Insolvency/Resolution**

### **52.1 Insolvency**

In the event that Bank becomes subject to insolvency proceedings, financial restructuring, or resolution by relevant authorities (including, but not limited to, governmental bodies, regulatory agencies, or liquidators), the Service Provider shall cooperate fully with such authorities, in accordance with applicable laws and regulations.

### **52.2 Cooperation**

The Service Provider agrees to provide all necessary information, documentation, and assistance as requested by the relevant authorities, including but not limited to access to data, records, systems, and personnel, to ensure a smooth transition or orderly resolution process.

### **52.3 Continued Service During Resolution**

In the event of insolvency or resolution of the Bank, the Service Provider shall continue to perform its obligations under this Agreement unless otherwise directed by the relevant authorities or instructed by Bank.

### **52.4 Notification**

The Service Provider shall notify the Bank promptly upon learning of any insolvency, liquidation, or resolution proceedings involving the Bank, and shall comply with any directions provided by the relevant authorities.

## **53 Data Localization**

The Bidder shall ensure that all data, as applicable to the concerned Bank, is stored exclusively within India, in full compliance with the extant regulatory requirements set forth by the relevant authorities. The Bidder shall not store or process any data outside of India without prior written consent from the Bank and approval from regulatory bodies.

**54 Authorized Signatory**

The Bidder shall indicate the authorized signatories who can discuss and correspond with Bank, with regard to the obligations under the contract. The Bidder shall submit at the time of signing the contract a certified copy of the resolution of their board, authenticated by the company secretary, authorizing an official or officials of the bidder to discuss, sign agreements/contracts with Bank, raise invoice and accept payments and also to correspond. The Bidder shall provide proof of signature identification for the above purposes as required by Bank.

**55 Escrow Arrangements**

The bidder has to facilitate for Escrow Agreement between all the parties. The OEM shall either provide the source code along with the necessary documentation or ensure that the source code is securely placed under an escrow arrangement, as agreed upon by all parties. The escrow agreement shall include provisions that, in the event of a predefined triggering event (such as the OEM going out of business, breach of contract, or any other specified event), the source code will be made available to the Bank in a timely manner, ensuring uninterrupted support and maintenance of the solution.

The Bidder shall bear all costs related to setting up and maintaining the escrow arrangement, including any charges incurred for the services of the Escrow Agent. The Bank shall not be responsible for any costs related to the escrow setup or the escrow agent's services.

In addition, the Service Provider shall ensure regular and secure backups of the source code and other critical data. Backup of all relevant data, including the source code, must be performed and securely stored in accordance with the Bank's Data Security and compliance requirements. The Bank shall have access to these backups upon request to ensure continuity and security of operations.



# **Section-4**

## **Annexures**

### Checklist for Submission

#	Particulars	Bidders Remark (Yes/No)
1	Certificate of Incorporation	
2	Audited Balance sheets of last three years - 2021-22, 2022-23, 2023-24	
3	CA certificate for three years average turnover for financial years 2021-22, 2022-23, 2023-24	
4	CA certificate for operating profit for last three financial years 2021-22, 2022-23, 2023-24	
5	CA certificate for net worth for last three financial years i.e. 2021-22, 2022-23, 2023-24	
6	Self-declaration by the Authorized Signatory for not having filed for Bankruptcy in any country including India on company letter head	
7	Self-declaration on Company's letter head stating bidder should not have been blacklisted/debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason or non-implementation/ delivery of the order.	
8	Self-declaration on Company's letter head stating Bidder/OEM should not have any pending litigation or any dispute in the last 5 years	
9	Self-declaration on Company's letter head regarding • NPA • Any case pending	
10	Document Cost	
11	Annexure 1: Conformity Letter	
12	Annexure 2: Commercial Bill of Material	
13	Annexure 3: Bidder's Information	
14	Annexure 4: Letter for Conformity of Product as per RFP	
15	Annexure 5: GOI Guidelines with Model wise classification (Make in India)	
16	Annexure 6: Undertaking of Authenticity for Products Supplied	
17	Annexure 7: Undertaking for Acceptance of terms of RFP	
18	Annexure 8: MAF on OEM letter head	
19	Annexure 9: Integrity Pact	
20	Annexure 10: Non-Disclosure Agreement	
21	Annexure 11: Performance Bank Guarantee	
22	Annexure 12: Minimum Technical Specifications	
23	Annexure 13: Pro forma for Bid Security (EMD)	
24	Annexure 14: Bidders Particulars in Company Letter Head	
25	Annexure 15: Compliance Certificate with respect to RBI's "Master Direction on Outsourcing of Information Technology Services"	
26	Annexure 16: NPA Undertaking	
27	Annexure 17: Land Border Sharing Undertaking	
28	Annexure 18: Cover Letter	
29	Annexure 19: Escalation Matrix	
30	Annexure 20: Query Format	
31	Annexure 21: Eligibility Criteria Compliance	
32	Annexure 22: Guidelines on banning of Business Dealings	
33	Annexure 23: Undertaking of Information Security from Bidder	
34	Annexure 24: Software Bill of Material (SBOM) Format	
35	Annexure 25- Template for Third Party Due Diligence Questionnaire	

## **Annexure 1: Conformity Letter**

Date

To,

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

Sir,

Sub: Tender No. GEM/2025/B/6170727

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

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

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

Yours faithfully,

Authorized Signatory

Designation

Company Name

**Annexure 2: Commercial Bill of Material**

Format for Commercial Bill of Material is attached in excel format in separate sheet and also provide at the end of this RFP.

**Annexure 3: Bidder's Information**

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

Signature

Name:

Designation:

Seal of Company

Date:

#### **Annexure 4: Letter for Conformity of Product as per RFP**

Date

To,

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

Sir,

Sub: Tender No. GEM/2025/B/6170727

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

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

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

<b>Compliance</b>	<b>Compliance (Yes/ No)</b>	<b>Remarks</b>
Terms & Conditions		
Scope of Work		

(If left blank it will be construed that there is no deviation from the specifications given above)

Signature

Name:

Designation:

Seal of Company

Date:

### **Annexure 5: GOI Guidelines with Model wise classification (Make in India)**

Government has issued Public Procurement (Preference to Make in India) [PPP-MII] Order 2017 vide the Department for Promotion of Industry and Internal Trade (DPIIT) Order No.P45021/2/2017-B.E.-II dated 15.06.2017 and subsequent revisions vide Order No. 45021/2/2017-PP(BE-II) dated 16-9-2020 to encourage 'Make in India' and to promote manufacturing and production of goods, services and works in India with a view to enhancing income and employment.

It is clarified that for all intents and purposes, the latest revised order i.e. the order dated 16-9-2020 shall be applicable being revised Order of the original order i.e. Public Procurement (Preference to Make in India) [PPP-MII] Order 2017 dated 15-6-2017.

The salient features of the aforesaid Order are as under:

- 1) Class-I Local supplier - a supplier or service provider, whose goods, services or works offered for procurement, has local content equal to or more than 50%.
- 2) Class-II Local supplier - a supplier or service provider, whose goods, services or works offered for procurement, has local content equal to or more than 20% but less than 50%.
- 3) Non-Local supplier - a supplier or service provider, whose goods, services or works offered for procurement, has local content less than or equal to 20%.
- 4) The margin of purchase preference shall be 20 %., Margin of purchase preference means the maximum extent to which the price quoted by a local supplier may be above the L1 for the purpose of purchase preference.
- 5) "Minimum Local content" for the purpose of this RFP, the 'local content' requirement to categorize a supplier as 'Class-I local supplier' is minimum 50%. For 'Class-II local supplier', the 'local content' requirement is minimum 20%. If Nodal Ministry/Department has prescribed different percentage of minimum 'local content' requirement to categorize a supplier as 'Class-I local supplier'/'Class-II local supplier', same shall be applicable.

Verification of Local contents:

The local supplier at the time of submission of bid shall be required to provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content as per Annexure 5A. Local content certificate shall be issued based upon the procedure for calculating the local content /domestic value addition on the basis of notification bearing no. F. No.33(1) /2017-IPHW dated 14-9-2017 issued by Ministry of Electronics and Information Technology read with Public Procurement (Preference to Make in India) Order 2017 Revised vide the Department for Promotion of Industry and Internal Trade (DPIIT) Order No.P-45021/2/2017-B.E.-II dated 16-09-2020.

False declaration will be in breach of the Code of Integrity under Rule 175(i)(h) of the General Financial Rules for which a bidder or its successors can be debarred for up to two years as per rule 151 of the General Financial Rules along with such other actions may be permissible under law.

A supplier who has been debarred by any procuring entity for violation of this order shall not be eligible for preference under this order for procurement by any other procuring entity for the duration of the debarments. The debarment for such other procuring entities shall take effect prospectively from the date on which it comes to the notice of other procurement entities in the manner prescribed under order No P-45021/2/2017-PP(BE-II) dated 16-092020, para 9(h).

Note:

- a) Bidder has to submit the Make in India Class-I / Class-II local supplier certificate as per attached format.
- b) Bidder has to submit proposal for all line Items.
- c) Any change in classification of Class-I and Class-II, Bidder may submit any change in class level for consideration in subsequent phases.

Purchase Preference:

- 1) Subject to the provisions of this Order and to any specific instructions issued by the Nodal Ministry or in pursuance of this Order, purchase preference shall be given to 'Class-I local supplier' in procurements undertaken by procuring entities in the manner specified here under,
- 2) In the procurements of goods or works, which are divisible in nature, the 'Class-I local supplier' shall get purchase preference over 'Class-II local supplier' as well as 'Non-local supplier', as per following procedure:
  - Among all qualified bids, the lowest bid will be termed as L1. If L1 is 'Class-I local supplier', the contract for full quantity will be awarded to L1.
  - If L1 bid is not a 'Class-I local supplier', 50% of the order quantity shall be awarded to L1. Thereafter, the lowest bidder among the 'Class-I local supplier' will be invited to match the L1 price for the remaining 50% quantity subject to the Class-I local supplier's quoted price falling within the margin of purchase preference, and contract for that quantity shall be awarded to such 'Class-I local supplier' subject to matching the L1 price. In case such lowest eligible 'Class-I local supplier' fails to match the L1 price or accepts less than the offered quantity, the next higher 'Class-I local supplier' within the margin of purchase preference shall be invited to match the L1 price for remaining quantity and so on, and contract shall be awarded accordingly. In case some quantity is still left uncovered on Class-I local suppliers, then such balance quantity may also be ordered on the L1 bidder.
- 3) In the procurements of goods or works, which are not divisible in nature, and in procurement of services where the bid is evaluated on price alone, the 'Class-I local supplier' shall get purchase preference over 'Class-II local supplier' as well as 'Non-local supplier', as per following procedure:
  - Among all qualified bids, the lowest bid will be termed as L1. If L1 is 'Class-I local supplier', the contract will be awarded to L1.
  - If L1 is not 'Class-I local supplier', the lowest bidder among the 'Class-I local supplier', will be invited to match the L1 price subject to Class-I local supplier's



quoted price falling within the margin of purchase preference, and the contract shall be awarded to such 'Class-I local supplier' subject to matching the L1 price.

- In case such lowest eligible 'Class-I local supplier' fails to match the L1 price, the 'Class- I local supplier' with the next higher bid within the margin of purchase preference shall be invited to match the L1 price and so on and contract shall be awarded accordingly. In case none of the 'Class-I local supplier' within the margin of purchase preference matches the L1 price, the contract may be awarded to the L1 bidder.
- 4) "Class-2 local supplier" will not get purchase preference in any procurement, undertaken by procuring entities.

All others terms and condition are as per order no. No. P-45021/2/2017-PP (BE-II) dated: 16th September 2020.

#### **Annexure 5A: Certificate of Local Content**

(Certificate from the statutory auditor or cost auditor of the company (in case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content, on their letter head with Registration Number with seal)

To,

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

Sir,

Sub: Tender No. GEM/2025/B/6170727

This is to certify that proposed ..... (product make\_\_\_\_ and model\_\_\_\_) is having the local content of ..... % as defined in the above mentioned RFP.

This certificate is submitted in reference to the Public Procurement (Preference to Make in India), Order 2017.

## **Annexure 6: Undertaking of Authenticity for Products Supplied**

Date

To,

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

Sir,

Sub: Tender No. GEM/2025/B/6170727

With reference to RFP for -----:

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

In case of default and we are unable to comply with the above at any time, we agree to take back the Licenses without demur, if already supplied and return the money if any paid to us by you in this regard.

Signature

Name:

Designation:

Seal of Company

Date:

## **Annexure 7: Undertaking for Acceptance of Terms of RFP**

Date

To,

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

Sir,

Sub: Tender No. GEM/2025/B/6170727

With reference to RFP for -----:

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

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

Signature

Name:

Designation:

Seal of Company

Date:

## **Annexure 8: Manufacturer's Authorization Form**

Date

To,

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

Dear Sir,

Sub: Tender No. GEM/2025/B/6170727

We ..... (Name of the Manufacturer)  
who are established and reputable manufacturers of ..... having  
factories at ....., ....., ....., ..... and ..... do hereby authorize M/s  
..... (who is the Bidder submitting its bid pursuant to the Request for  
Proposal issued by the Bank) to submit a Bid and negotiate and conclude a contract with you  
for supply of equipment manufactured by us against the Request for Proposal received from  
your Bank by the Bidder and we have duly authorized the Bidder for this purpose.

We, hereby, extend warranty for the equipment and support services offered for our products  
supplied against this RFP by the above-mentioned Bidder.

If Bank desires transfer of the warranty and support services, supposed to be delivered by the  
successful Bidder, to its preferred Bidder, in such a case, OEM should transfer such warranty  
and support services without any additional cost to the Bank.

Yours Faithfully,

Authorized Signatory

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

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

## **Annexure 9: Integrity Pact**

Integrity Pact

Between

Central Bank of India hereinafter referred to as “The Principal”,

And

..... hereinafter referred to as “The Bidder/  
Contractor”

### **Preamble**

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

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

### **Section 1 – Commitments of the Principal**

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

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

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

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

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

- a. The Bidder(s)/ Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principal’s employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she

is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

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

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

d. The Bidder(s)/Contractors(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly, the Bidder(s)/Contractors(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the “Guidelines on Indian Agents of Foreign Suppliers” shall be disclosed by the Bidder(s)/Contractor(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only. Copy of the “Guidelines on Indian Agents of Foreign Suppliers” is placed at Annexure 22.

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

f. Bidder(s)/Contractor(s) who have signed the Integrity Pact shall not approach the Courts while representing the matter to IEMs and shall wait for their decision in the matter

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

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

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the procedure mentioned in the “Guidelines on Banning of business dealings”. Copy of the “Guidelines on Banning of business dealings”. (As given in the Annexure 22)

### **Section 4 – Compensation for Damages**

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

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

### **Section 5 – Previous Transgression**

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

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

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

(1) The Bidder(s)/ Contractor(s) undertake(s) to demand from his subcontractors a commitment in conformity with this Integrity Pact.

(2) The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.

(3) The Principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

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

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

#### **Section 8 – Independent External Monitor / Monitors**

- 1) The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.
- 2) The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. It will be obligatory for him to treat the information and documents of the Bidders/Contractors as confidential. He reports to the Chairman & Managing Director, CENTRAL BANK OF INDIA.
- 3) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/ Subcontractor(s) with confidentiality. In case of sub-contracting, the Principal Contractor shall take all responsibility of the adoption of Integrity Pact by the sub-contractor. In case of sub-contracting, the Principal Contractor shall take the responsibility of the adoption of the Integrity Pact by the sub-contractor.
- 4) The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.
- 5) As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to

discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit nonbinding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action. Parties to this agreement agree that they shall not approach the courts while representing the matter to IEM and will await IEM's decision in the matter. Parties to this agreement agree that they shall not approach the courts while representing the matter to IEM and will await IEM's decision in the matter.

- 6) The Monitor will submit a written report to the Chairman & Managing Director, CENTRAL BANK OF INDIA within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.
- 7) If the Monitor has reported to the Chairman & Managing Director CENTRAL BANK OF INDIA, a substantiated suspicion of an offence under relevant IPC/ PC Act, and the Chairman & Managing Director CENTRAL BANK OF INDIA has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.
- 8) The word „Monitor“ would include both singular and plural.

### **Section 9 – Pact Duration**

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

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

### **Section 10 – Other provisions**

- 1) This agreement is subject to Indian Law. Place of performance and jurisdiction is the Registered Office of the Principal, i.e. Mumbai.
- 2) Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.
- 3) If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.
- 4) Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.
- 5) In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the Integrity Pact will prevail.”

### **Section 11- FALL CLAUSE**

**11.1.** The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER undertakes that it has not supplied/is not supplying same/exact product/systems or subsystems/services (i.e. same scope, deliverables, timelines, SLAs & pricing terms) at a price lower than that offered in the present bid to any other Bank or PSU or Government Department or to any other organization/entity whether or not constituted under any law and if it is found at any



stage that similar product/systems or sub systems/services was supplied by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER to any other Bank or PSU or Government Department or to any other organization/entity whether or not constituted under any law, at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER to the BUYER, if the contract has already been concluded.

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

## **Annexure 10: Non-Disclosure Agreement**

This Agreement made at \_\_\_\_\_, on this \_\_\_\_ day of \_\_\_\_\_ 2025

Between

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

AND

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

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

WHEREAS:

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

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

### **1. Confidential Information**

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

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

Notwithstanding the foregoing, “Confidential Information” shall not include any information which the Receiving Party can show: (a) is now or subsequently becomes legally and publicly available without breach of this Agreement by the Receiving Party, (b) was rightfully in the possession of the Receiving Party without any obligation of confidentiality prior to receiving it from the Disclosing Party, (c) was rightfully obtained by the Receiving Party from a source other than the Disclosing Party without any obligation of confidentiality, or (d) was developed

by or for the Receiving Party independently and without reference to any Confidential Information and such independent development can be shown by documentary evidence.

## **2. Non-Disclosure**

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

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

## **3. Publications**

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

## **4. Term**

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

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

## **5. Title & Proprietary Rights**

Notwithstanding the disclosure of any Confidential Information by the Disclosing Party to the Receiving Party, the Disclosing Party shall retain title and all intellectual property and proprietary rights in the Confidential Information. No license under any trademark, patent or

copyright, or application for same which are now or thereafter may be obtained by such Party is either granted or implied by the conveying of Confidential Information. The Receiving Party shall not conceal, alter, obliterate, mutilate, deface or otherwise interfere with any trademark, trademark notice, copyright notice, confidentiality notice or any notice of any other proprietary right of the Disclosing Party on any copy of the Confidential Information, and shall reproduce any such mark or notice on all copies of such Confidential Information. Likewise, the Receiving Party shall not add or emboss its own or any other any mark, symbol or logo on such Confidential Information.

## **6. Return of Confidential Information**

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

## **7. Remedies**

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

## **8. Entire Agreement, Amendment and Assignment**

This Agreement constitutes the entire agreement between the parties relating to the matters discussed herein and supersedes any and all prior oral discussions and/or written correspondence or agreements between the parties. This Agreement may be amended or modified only with the mutual written consent of the parties. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable.

## **9. Governing Law and Jurisdiction**

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

## **10. General**

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

## **11. Indemnity**

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

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

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

## **Annexure 11: Performance Bank Guarantee**

To,

Central Bank of India, Mumbai

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

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

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

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

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

5) In order to give full effect to the Guarantee herein contained, you shall be entitled to act as if we are your principal debtors in respect of all your claims against the contractor hereby Guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights if any which are in any way inconsistent with the above or any other provisions of this Guarantee.

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

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

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

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

10) Notwithstanding anything contained herein:-

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

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

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

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

Date this ----- day of ----- 2025 at -----

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

sd/- -----

## **Annexure 12: Minimum Technical Specifications**

Format for Minimum Technical Specifications is attached in excel format in separate sheet and also provide at the end of this RFP.



### Annexure 13: Bid Security (BG Format- for Earnest Money Deposit)

To,

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

Dear Sir,

In response to your invitation to respond to your RFP for \_\_\_\_\_, M/s \_\_\_\_\_ having their registered office at \_\_\_\_\_ (hereinafter called the Bidder“) wishes to respond to the said Request for Proposal (RFP) and submit the proposal for as listed in the RFP document.

Whereas the „Bidder“ has submitted the proposal in response to RFP, we, the \_\_\_\_\_ Bank having our head office \_\_\_\_\_ hereby irrevocably guarantee an amount of **Rs \_\_\_\_\_ (Rupees .....Only)** as bid security as required to be submitted by the, Bidder“ as a condition for participation in the said process of RFQ.

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

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

Notwithstanding anything contained herein:

1. Our liability under this Bank guarantee shall not exceed **Rs. \_\_\_\_\_ (Rupees .....Only)**
2. This Bank guarantee will be valid up to \_\_\_\_\_; and
3. We are liable to pay the guarantee amount or any part thereof under this Bank

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

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

Yours faithfully,

For and on behalf of \_\_\_\_\_

Bank Authorised Official

**Annexure 14: Bidder's Particulars**

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

Signature

Name:

Designation:

Seal of Company

Date:

**Annexure 15: Compliance Certificate with respect to RBI's "Master Direction on Outsourcing of Information Technology Services"**

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

Date:-----

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

**Subject: RFP for Augmentation / Refresh of Patch Management Solution, Active Directory (AD) Management Solution and Procurement of related System Software"**

Sir,

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

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

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

Authorized Signatory Name:

Designation:

Email and Phone

## **Annexure 16: NPA UNDERTAKING**

Performa of letter to be given by all the bidders participating in RFP for Augmentation, Refresh of System Supporting Application at Bank on their official letter-head

Date:

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

**Subject: RFP for Augmentation / Refresh of Patch Management Solution, Active Directory (AD) Management Solution and Procurement of related System Software”**

We \_\_\_\_\_(bidder name), hereby undertake that-

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

Yours faithfully,

Authorised Signatory

Designation

Bidder's corporate name

**Annexure17: Land Border Sharing Undertaking Letter**

Pro forma of letter to be given by all the bidders participating in the RFP for Augmentation, Refresh of System Supporting Application at Bank on their official letter-head

To

Date:

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

Sir,

**Sub: RFP for Augmentation / Refresh of Patch Management Solution, Active Directory (AD) Management Solution and Procurement of related System Software”**

**Dear Sir/Madam,**

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

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

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

Strike off whichever is not applicable

1. “I/we have read the clause regarding restrictions on procurement from a bidder of the country which shares a land border with India; I/ we certify that \_\_\_\_\_ is not from such a country.
2. “I/we have read the clause regarding restrictions on procurement from a Bidder of a country which shares a land border with India; I/we certify that \_\_\_\_\_ is from such a country. I hereby certify that \_\_\_\_\_ fulfils all requirements in this regard and is eligible to be considered. [Valid registration by the Competent Authority is attached]”

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

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

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

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

Dated this \_\_\_\_\_ by \_\_\_\_\_ 20\_\_

Yours faithfully,

Authorized Signatory

Name:

Designation:

Bidder's Corporate Name:

Address:

Email & Phone No.:

List of documents enclosed:

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

**Annexure 18: Cover Letter**

Date:

To

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

**Dear Sir/Madam,**

1. Having examined the Scope Documents including all Annexures, the receipt of which is hereby duly acknowledged, we, the undersigned offer to supply, deliver, install and maintain all the items mentioned in the 'Request for Proposal' and the other schedules of requirements and services for your Bank in conformity with the said Scope Documents in accordance with the schedule of Prices indicated in the Price Bid and made part of this Scope.
2. If our Bid is accepted, we undertake to abide by all terms and conditions of this Scope and also to comply with the delivery schedule as mentioned in the Scope Document.
3. We agree to abide by this bid Offer for 180 days from date of bid (Commercial Bid) opening and our Offer shall remain binding on us which may be accepted by the Bank any time before expiry of the offer.
4. This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.
5. We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".
6. We certify that we have provided all the information requested by the Bank in the format prescribed for. We also understand that the Bank has the exclusive right to reject this offer in case the Bank is of the opinion that the required information is not provided or is provided in a different format.

Authorised Signatory

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

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

## Annexure 19: [Escalation Matrix]

Ref: Tender No - GEM/2025/B/6170727

Date: -

To  
The General Manager-IT  
Department of Information Technology  
Central Bank Of India  
Plot No -26, Sector-11, CBD Belapur-400614, Navi Mumbai

Sir,

**Reg: RFP for Augmentation / Refresh of Patch Management Solution, Active Directory (AD) Management Solution and Procurement of related System Software**

Escalation Matrix.

### Name of the Company

#### Delivery Related Issues:

Sr .	Name	Designation	Full Office Address	Phone No.	Mobile	Email address
A		First Level Contact				
B		Second level Contact				
C		Third level Contact				
D		Country Head				

#### Service Related Issues:

Sr .	Name	Designation	Full Office Address	Phone No.	Mobile	Email address
a		First Level Contact				
b		Second level Contact				
c		Third level Contact				
d		Country Head				

Any change in designation, substitution will be informed by us immediately.

(Signature of the Bidder with Seal)

Full name and Designation of authorized signatory

Date:

Phone No.:

E-mail:



## Annexure 20: Query Format

Queries:

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

Date:

Authorised Signatory & Stamp

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

## Annexure 21: Eligibility Criteria Compliance

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

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

#	Eligibility of the Bidder and OEM	Documents to be submitted	Compliance (Y/N)
<b>Bidder's Financial Strength</b>			
1.	Bidder should be a Registered company under Indian Companies Act. 1956/2013 or LLP/Partnership firm and should have been in existence for a minimum period of 5 years in India, as on date of submission of RFP.	Copy of the Certificate of Incorporation issued by Registrar of Companies/Registrar of firms and full address of the registered office of the bidder	
2.	Bidder should be registered under G.S.T and/or tax registration in state where bidder has a registered office	Proof of registration with GSTIN	
3.	The bidder must have an annual turnover in India of INR 150 Crores per annum in the last three financial years (i.e. 2021-22, 2022-23, 2023-24).	Copy of audited Balance Sheet and Certificate of the Chartered Accountant for preceding three FYs.	
4.	The bidder should have made operating profits in at least two financial years out of last three financial years. (i.e. 2021-22, 2022-23, 2023-24).	Copy of audited Balance Sheet and Certificate of the Chartered Accountant for preceding three FYs.	
5.	The bidder should have a positive net worth in last three financial years (i.e. 2021-22, 2022-23, 2023-24)	Certificate of the Chartered Accountant for preceding three FYs.	
<b>Bidder and OEM Experience</b>			
6.	The Bidder should be a certified or an Authorized partner of the OEM of the offered solution	Copy of MAF from OEMs as per format (Annexure 8) to be submitted, and confirmation from OEMs confirming the	

#	Eligibility of the Bidder and OEM	Documents to be submitted	Compliance (Y/N)
		partnership level of the Bidder	
7.	Bidder/ OEMs should have service/ support infrastructure at Mumbai/ Hyderabad and should be able to provide efficient and effective support.	Submit the undertaking self-declaration on Bidder's and OEM's letter head	
8.	<p>Bidder should have experience of having implemented or provided Support for</p> <ul style="list-style-type: none"> <li>Active Directory Management Solution</li> </ul> <p>OR</p> <ul style="list-style-type: none"> <li>Patch Management Solution,</li> </ul> <p>in at least one Scheduled Commercial Bank / BFSI /PSU in India in last 5 years having minimum 1000 Office/Branches in India.</p>	<p>Credential letter OR</p> <p>Copy of</p> <p>Purchase order/ Contract copy</p>	
9.	<p>The OEM for each Proposed Product should have been implemented in at least One Scheduled Commercial Bank/BFSI having minimum 1000 Office/Branches in India in last 5 years.</p> <ol style="list-style-type: none"> <li>Active Directory Management Solution</li> <li>Patch Management Solution,</li> <li>SFTP Solution</li> <li>Load Balancer</li> </ol>	<p>Credential letter OR</p> <p>Copy of</p> <p>Purchase order/ Contract copy</p>	
<b>Bidders Compliance</b>			
10.	At the time of bidding, the Bidder should not have been blacklisted/debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason or non-implementation/ delivery of the order. Self-declaration to that effect should be submitted along with the technical bid.	Submit the undertaking self-declaration on Company's letter head	
11.	At the time of bidding, there should not have been any pending litigation or any legal dispute in the last five years, before any court of law between the Bidder or OEM and the Bank regarding supply of goods/services	Submit the undertaking self-declaration on Company's letter head	
12.	<p>Bidder/OEM should not have -</p> <ul style="list-style-type: none"> <li>NPA with any Bank /financial institutions in India</li> </ul>	Submit self-declaration on Company's letter head.	

#	Eligibility of the Bidder and OEM	Documents to be submitted	Compliance (Y/N)
	<ul style="list-style-type: none"> <li>Any case pending or otherwise, with any organization across the globe which affects the credibility of the Bidder in the opinion of Central Bank of India to service the needs of the Bank</li> </ul>		
13.	If the bidder is from a country which shares a land border with India, the bidder should be registered with the Competent Authority	Certified copy of the registration certificate	

The bidder must submit only such document as evidence of any fact as required herein. The Bank, if required, may call for additional documents during the evaluation process and the bidder will be bound to provide the same.

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

- 1) Bidders need to ensure compliance to all the eligibility criteria points.
- 2) In-case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.
- 3) In case of business transfer where Bidder has acquired a Business from an entity ("Seller"), work experience credentials of the Seller in relation to the acquired business may be considered.
- 4) Purchase orders without relevant organization confirmation through a credential letter will not be considered as credentials.
- 5) If an agent submits a bid on behalf of the Bidder/ OEM, the same agent shall not submit a bid on behalf of another Principal/ OEM for the same solution.
- 6) Scheduled Commercial Bank does not include Payments Bank, Cooperative Banks or RRBs.
- 7) While submitting the bid, the Bidder is required to comply with inter alia the following CVC guidelines detailed in Circular No. 03/01/12 (No.12-02-6 CTE/SPI (I) 2 / 161730 dated 13.01.2012): 'Commission has decided that in all cases of procurement, the following guidelines may be followed:
  - i. *In RFP, either the Indian agent on behalf of the Bidder/OEM or Bidder/OEM itself can bid but both cannot bid simultaneously for the same item/product in the same RFP. The reference of 'item/product' in the CVC guidelines refer to 'the final solution that bidders will deliver to the customer.'*
  - ii. *If an agent submits bid on behalf of the Bidder /OEM, the same agent shall not submit a bid on behalf of another Bidder /OEM in the same RFP for the same item/product.'*

Authorised Signatory

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

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

## **Annexure 22: Guidelines on Banning of Business Dealing**

### **1.0 GUIDELINES FOR INDIAN AGENTS OF FOREIGN SUPPLIERS**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## **1. Introduction**

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

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

## **2. Scope**

2.1 The General Conditions of Contract (GCC) of CENTRAL BANK OF INDIA generally provide that CENTRAL BANK OF INDIA reserves its rights to remove from list of approved suppliers / contractors or to ban business dealings if any Agency has been found to have committed misconduct and also to suspend business dealings pending investigation. If such provision does not exist in any GCC, the same may be incorporated. 2.2. Similarly, in case of sale of material there is a clause to deal with the Agencies / customers/ Buyers, who indulge in lifting of material in unauthorized manner. If such a stipulation does not exist in any Sale Order, the same may be incorporated.

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

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

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

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

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

### **3. Definitions**

In these Guidelines, unless the context otherwise requires:

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



For procurement of items / award of contracts, to meet the requirement of Corporate Office only, Head of GAD shall be the “Competent Authority” and concerned Executive Director (GAD) shall be the “Appellate Authority”.

- v. Chairman & Managing Director, CENTRAL BANK OF INDIA shall have overall power to take suo-moto action on any information available or received by him and pass such order(s) as he may think appropriate, including modifying the order(s) passed by any authority under these guidelines.
- 4) ‘Investigating Department’ shall mean any Department or Unit investigating into the conduct of the Agency and shall include the Vigilance Department, Central Bureau of Investigation, the State Police or any other department set up by the Central or State Government having powers to investigate.
- 5) ‘List of approved Agencies - Parties / Contractors / Suppliers / Purchasers / Customers / Bidders / Tenderers shall mean and include list of approved / registered Agencies - Parties/ Contractors / Suppliers / Purchasers / Customers / Bidders / Tenderers, etc.

#### **4. Initiation of Banning / Suspension**

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

#### **5. Suspension of Business Dealings**

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

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

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

5.4 If the gravity of the misconduct under investigation is very serious and it would not be in the interest of CENTRAL BANK OF INDIA, as a whole, to deal with such an Agency pending investigation, the Competent Authority may send his recommendation to ED (GAD), CENTRAL BANK OF INDIA Corporate Office along with the material available. If Corporate Office considers that depending upon the gravity of the misconduct, it would not be desirable for all the Units and Subsidiaries of CENTRAL BANK OF INDIA to have any

dealings with the Agency concerned, an order suspending business dealings may be issued to all the Units by the Competent Authority of the Corporate Office, copy of which may be endorsed to the Agency concerned. Such an order would operate for a period of six months from the date of issue.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.11 Based on the findings of the investigation report of CBI / Police against the Agency for malafide / unlawful acts or improper conduct on his part in matters relating to the Bank (CENTRAL BANK OF INDIA) or even otherwise;

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

6.13 Continued poor performance of the Agency in several contracts;

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

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

## **7 Banning of Business Dealings**

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

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

- 1) To study the report of the Investigating Agency and decide if a prima-facie case for Bank- wide / Local unit wise banning exists, if not, send back the case to the Competent Authority.
- 2) To recommend for issue of show-cause notice to the Agency by the concerned department.
- 3) To examine the reply to show-cause notice and call the Agency for personal hearing, if required.
- 4) To submit final recommendation to the Competent Authority for banning or otherwise.

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

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

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

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

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

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

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

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

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

## **9 Show Cause Notice**

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

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

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

- i. For exonerating the Agency if the charges are not established;
- ii. For removing the Agency from the list of approved Suppliers / Contactors, etc.
- iii. For banning the business dealing with the Agency.

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

## **10 Appeal against the Decision of the Competent Authority**

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

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

## **11 Review of the Decision by the Competent Authority**

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

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

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

12.2 If Government Departments or a Public Sector Enterprise request for more information about the Agency with whom business dealings have been banned, a copy of the report of Inquiring Authority together with a copy of the order of the Competent Authority / Appellate Authority may be supplied.

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

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

## **Annexure 23: [Undertaking of Information Security from Bidder]**

Ref: Tender No - GEM/2025/B/6170727

Date: -

To,  
The General Manager-IT  
Department of Information Technology  
Central Bank Of India  
Plot No -26, Sector-11, CBD Belapur, Navi Mumbai-400614,

Sir,

**Reg:- RFP for Augmentation / Refresh of Patch Management Solution, Active Directory (AD) Management Solution and Procurement of related System Software**

We hereby undertake that the proposed product to be supplied will be free of malware, free of any obvious bugs and free of any covert channels in the code (of the version of the software being delivered as well as any subsequent versions/modifications done) which may lead to any data leakage/compromise of the server/solution or any cyber security incident in future.

We also undertake that :-

- 1) The product offered, as part of the contract, does not contain Embedded Malicious Code that would activate procedures to:
  - i) Inhibit the desires and designed function of the equipment.
  - ii) Cause physical damage to the user or equipment during the exploitation.
  - iii) Tap information resident or transient in the equipment/network
- 2) The firm will be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and Intellectual Property Right (IPRs) are caused due to activation of any such malicious code in embedded software and any loss occurring due to the above may be recovered from the existing contracts.
- 3) To ensure that the setup / link provided for updation / downloading / authorisation of licenses either on Banks network or through Internet should be free of any malware / viruses etc. Any damages / losses caused to Bank due to aforesaid shall be passed on to the bidder account.

Yours faithfully,

(Signature of the Bidder with Seal)  
Full name and Designation of authorized signatory  
Date:  
Phone No.: E-mail:

**Annexure 24: [Software Bill of Material (SBOM) Format]**

<b>SBOM FORMAT</b>								
<b>S N</b>	<b>Applica tion Name</b>	<b>Softw are Packa ges</b>	<b>Type of Software ( App/Web/DB /Middleware)</b>	<b>Installed Version/ Installed Date</b>	<b>Late st Vers ion</b>	<b>License Type ( Perpetu al/ Subscri ption )</b>	<b>No. of Licenses/ AMC validity</b>	<b>OEM/ AMC Vendo r</b>
1								
2								
3								
4								

The bidder must submit only such document as assurance regarding the accuracy, completeness and timelines of SBOM.

Yours faithfully,

(Signature of the Bidder with Seal)  
Full name and Designation of authorized signatory  
Date:

### Annexure 25- Template for Third Party Due Diligence Questionnaire

<b>Third Party Name</b>					
<b>Third Party Location</b>					
<b>Service Description</b>					
<b>S. N.</b>	<b>Domain</b>	<b>Sub-domain</b>	<b>Control question</b>	<b>Response</b>	<b>Comments (If any)</b>
				<b>(To be filled by Third Party)</b>	
1	Governance	Strategy & Operating Model	Do you have a dedicated information / cyber security team, responsible for information security governance across the organization?		
2	Governance	Policies, Standards & Architecture	Do you have information / cyber security policy?		
3	Governance	Policies, Standards & Architecture	Are all your policies and procedures reviewed periodically?		
4	Governance	Cyber Risk Culture & Behaviour	Do you perform periodic risk assessments? If Yes, please define the frequency		
5	Governance	Cyber Risk Management, Metrics & Reporting	Is your environment ISO 27001: 2013 certified for the scope of the service being offered to Central Bank of India? If Yes, please provide the latest copy of the certification and specify the scope of implementation.		
6	Governance	Cyber Risk Management, Metrics & Reporting	Is your environment SOC 2 Type II attested or certified for the scope of the service being offered to Central Bank of India?		
7	Governance	Cyber Risk Management, Metrics & Reporting	Is your environment PCI - DSS certified for the scope of the service being offered to Central Bank of India?		
8	Governance	Cyber Risk Management, Metrics & Reporting	Are appropriate procedures & controls implemented to ensure compliance with the usage of proprietary software products?		
9	Resilient	Incident & Crisis Readiness	Do you have a formal document for incident management?		
10	Resilient	Incident & Crisis Readiness	Is awareness training given to your employees to identify information security events?		
11	Resilient	Incident & Crisis Readiness	Do you have a formal cyber crisis management plan?		



12	Resilient	Incident Response	a. Have you ever experienced a cybersecurity incident or data breach in last 3 years? This includes network, systems, software, etc. b. Will you notify Central Bank of India about any security, privacy incident, and event of disaster affecting Central bank of India services within 2 hrs. of incident being identified? c. Are the root cause analysis is performed for the security incidents.		
13	Resilient	Incident Response	Please provide details if you have ever been subject to any enforcement actions, investigations or litigation related to privacy or information security?		
14	Resilient	BCP / DR	Do you have a Business Continuity / Disaster Recovery Plan in place at an organization level?		
15	Resilient	BCP / DR	Have you identified the events that could cause interruptions to business process?		
16	Resilient	BCP / DR			
17	Resilient	BCP / DR	Do you have a failover site? Please describe if that is Hot, Warm or Cold site.		
18	Resilient	BCP / DR	Is there sufficient redundant capacity to ensure services are not impacted in multi-tenant environments during peak usage?		
19	Resilient	BCP / DR	If You store Central Bank of India data - is backed up data tested on a regular basis? - is data backup encrypted?		
20	Information Security	Penetration Testing & Vulnerability Scanning	Do you periodically perform External IS Audit/ VAPA		
21	Information Security	Security Event Monitoring	1. Do you have mechanism to preserve Audit trail logs?		
22	Information Security	Network Security	Have you implemented Advance cyber security controls/ tools (eg. WAF, DDoS, Firewall , SIEM etc)		
23	Information Security	Customer Data Protection	Do you have the technical capabilities to identify & segregate Central Bank of India's data [including Bank's customer data] from other entities data and maintain confidentiality & integrity? Please describe and share the evidence.		

24	Ethics, Regulatory & Compliance	Ethics, Regulatory & Compliance	Has the third-party or has any of the third-party's owners directors/ shareholders/employees been the subject of any allegations, investigation, conviction and/or other relevant criminal practices relating to bribery or corruption in the last three years?		
25	Ethics, Regulatory & Compliance	Ethics, Regulatory & Compliance	Has the third-party complied with all applicable provisions of HR-related Acts, including, but not limited to Contract Labour (Regulation & Abolition) Act, Minimum Wages Act, Payment of Wages Act, Maternity Benefits Act, Payment of Gratuity Act, Equal Remuneration Act, Employee's Compensation Act, etc.?		
26	Ethics, Regulatory & Compliance	Ethics, Regulatory & Compliance	In the last three years has the third-party received any local/governmental citations or fines relating to labour issues?		
27	Data Privacy	Monitoring & Enforcement	Do you have Adequate data privacy and security controls in place to protect data integrity and confidentiality.		
28	Data Privacy	Monitoring & Enforcement	Do you have and regular data privacy training and awareness module for your employees?		
29	Operational	HR/Personnel Security	Do you perform a background screening or check prior to allowing constituent access to systems and data ?		
30	Operational	Operation Management	Does the third-party have a defined process for tracking and ensuring compliance to SLAs / KPIs agreed with Central Bank of India?		
31	Operational	Operation Management	Are there adequate controls in place to monitor the activities undertaken through sub-contracting, including tracking of errors, etc.?		
32	Operational	Supply Chain Risk Management	Do you have documented & approved Organization level outsourcing risk management policy/framework to govern your third parties you are dependent upon?		
33	Operational	Supply Chain Risk Management	i. Have you obtained the prior consent from Central Bank of India for subcontracting complete or partial activities to third party[ies]		

34	Operational	Supply Chain Risk Management	Does your Agreement /Contract with your third parties who will be involved in provisioning/rendering services to Central Bank of India include a. Information/Data security/Regulatory requirements and applicable data security standards, privacy laws & data localization requirements b. Confidentiality c. Business Continuity d. Right to audit & seek information from the service provider.		
35	Strategic and Geographical	Country risk assessment	Do the third party provides service from India.		
36	Strategic and Geographical	Adverse Media	Has there been any adverse media published against the third party in past 2 years (relating to Financial Reporting, AML, Human Rights, Environmental Laws, Others etc.)). If Yes, please describe		
37	Financial Risk	Revenue Trend	Does the third party have a positive Net Worth/ Revenue Trend for last 3 financial years?		
38	Regulatory and Supervisory requirements		whether the service provider is located in India or abroad, the Service provide shall ensure that the outsourcing should neither impede nor interfere with the ability of the Bank to effectively oversee and manage the outsourcing activities. Further, the Service provide shall ensure that the outsourcing does not impede the RBI/ Auditor in carrying out its supervisory functions and objectives.		
39	Physical security	Physical & Environmental Security	a. Does vendor have physical and environmental security measures in place like CCTV, Fire extinguisher, fire alarm, Smoke detector, biometric, UPS, AC, etc. b. Is there regular fire drills performed?		

I /We hereby certified that the above information/data provided is correct and true. Bank can call for Evidence/ Documentary proof/ data in support of the above information for Audit / internal purpose anytime and the same will be provided and submitted to Bank as and when required

**Authorised Signatory**

**Name & Designation of Authorised Signatory**

## MINIMUM TECHNICAL SPECIFICATIONS

<b><u>Endpoint and Patch Management Solution</u></b>			
<b>S. N.</b>	<b>Technical Specification for Endpoint and Patch Management Solution</b>	<b>Bidder's Compliance (Yes/No)</b>	<b>Bidder's Remarks</b>
	<b>General</b>		
1	The solution should support patching for various operating systems (Windows, Linux etc) for desktops, laptops & servers.		
2	If any information or payload (e.g. Patch Metadata or Patch binaries) is downloaded from the internet, then the integrity of all such content must be verified by the solution using checksums to ensure that the content downloaded has not been modified or corrupted. File checksums and file sizes must be compared to make sure that the file is downloaded intact and unchanged.		
3	Centralize dashboard displaying overall count of devices part of bank IT infrastructure.		
4	The solution should provide ready-to-use patch management policies so that patch administrators can readily start patching the supported OS platforms using policy-based patching & customization.		
	<b>PATCH MANAGEMENT</b>		
1	Proposed Solutions must provide Windows Client Agent to allow administrators to quickly review the current state & perform actions to scan in one-click for any Client machines		
2	The proposed Solutions must be able to continuously assess and remediate while on or off the network related to patch management		
3	The Proposed Solutions must support the following OS platforms with agent, functionality coverage and Asset Management Solution: Windows, Linux OS (Redhat, CentOS, Ubuntu, SUSE) and other major OS systems in the market ( All Version)		
4	The proposed solutions should provide Granular filtering of software patches based on environmental requirements		
5	Proposed Solutions must provide Wake-on-LAN capabilities for device for after-hours maintenance regardless of location either using remote agent or from central console, Solutions must provide One-click software upgrades and Solutions must be able to Integrate with remote access software to control computer clients remotely to allow administrators to shut down, restart, hibernate, lock computers		
6	The solution should work over low-speed connections at remote sites.		
	<b>Patch Detection</b>		
1	The solution should provide out-of-box patch assessment without the need to schedule and maintain the patch or inventory scan process.		

2	The agent should report the assessment automatically within minutes once the server has distributed the new patch metadata/signatures.		
3	The solution shall use all of the following methods to determine if a patch has been installed on the client: i) Inspecting the registry. ii) Examining if the required files exist. iii) Inspecting the version number of existing files on the agent. OR iv) Any proprietary method (in addition to the patched OEM's specified method) to check the installation of the patch		
4	The solution should be able to determine patch dependencies prior to the deployment of patches to the desktop.		
5	The solution should be able to determine if a patch has already been installed on a desktop.		
6	The solution should be able to determine if a newer patch has been installed on the desktop and if so, the system shall treat the desktop as patched.		
	<b>Patch Deployment</b>		
1	The solution must provide the ability to group computers manually and dynamically based on asset and software information.		
2	Descriptions and severity levels of the patches shall be available within the Solution.		
3	All patches shall be tested based on standard practices before the patch information is made available and notifications shall be informed of any problems encountered during testing.		
4	The solution must allow the administrator to deploy patches to all computers or target specific computers to deploy the patches via a central console.		
5	The solution must allow the administrator to deploy patches without intervention from the users.		
6	The solution must allow the administrator to define different patch deployment policies & create custom policies.		
7	The solution must be able to provide real-time (within minutes) patch deployment status monitoring.		
8	The solution must allow administrator to deploy multiple patches at one time without the need to restart the computers.		
9	The solution must allow administrator to spread the patch deployment over a pre- defined period of time to reduce the overall impact on network bandwidth.		
10	Allow admin users to postpone the deployment of a patch for a period of time .		
11	Allow admin users to postpone the restarting of their computers for a period of time		
12	Able to re-deploy the patch on a computer automatically if the initial deployment is not successful or uninstalled by the user.		

13	The solution should support patching for a range of standard desktop applications from various vendors e.g. Microsoft, Google, Mozilla, Oracle, etc.		
14	Able to cache the patches in the various Distribution points.		
15	Able to install all previously deployed patches automatically to computers that are subsequently added to the network.		
16	Able to delete the patch installation files from the computers' hard disk automatically once the patch has been successfully applied.		
17	The administrator must be able to target the particular patch on all the machines with any specific properties.		
18	The tool should allow Testing of patch in UAT environment.		
19	The tool should allow deployment of emergency patches/urgent patches.		
20	The tool should allow updating the system patches automatically.		
	<b>Patch Rollback</b>		
1	Able to identify the computers that have installed the patch that is to be rolled back.		
2	Allow administrator to monitor the progress of the roll-back action from the central console.		
3	Able to report if the rollback is successful on the targeted computers.		
	<b>Software Distribution / Deployment</b>		
1	The proposed Solutions must provide patch management and distribution mechanism which should include OEM Supported Windows operating systems, industry-recognized Publishers of third-party software like Microsoft, Google, Mozilla, etc.		
2	The solution should be able for deployment of multiple packaging formats including EXE, MSI, InstallShield, and Batch.		
3	Should distribute third-party or in-house software to targeted computers.		
4	The solution should provide a wizard-driven approach to configure package information and target the applicability of the software distribution packages.		
5	Ability to create a 'Catalog Dashboard' that allows the end user to install any/all pre-defined software packages assigned.		
6	The Solutions must be supported for the deployment of patches at endpoints and servers having Low bandwidth		
7	<b>The proposed Solutions must be able to communicate with Linux update server e.g. Redhat, Suse etc. to take linux update for all supported Versions. Bidder should quote for Satellite Server licences if required for all the Linux systems of the Bank.</b>		

8	The Proposed Solutions must Verify the patch metadata produced by each content. It should Validate the patch installation and uninstallation processes along with it will confirm that the patch does not disrupt the stability of the targeted operating systems and applications. Proposed Solutions OEM should test and verify the patches on the below-mentioned parameters before being downloaded the to Central site to safe patches and save time in UAT testing and verification.a. The package is deployable.b. The suppress-reboot functionality works.c. The uninstallation functionality works.d. Automatic deployment scheduling works.		
9	The Solutions should provide wizard-based or silent, deployment or removal of software installed on inventory systems .		
10	The Proposed Solutions must be pre-integrated bundle of distributed management capabilities, operating environment and application software via a Web-based Solutions which is can be installed on VMware or Hyper-V or AHV Hypervisor over any Hardware and Solutions must provide web-based administration via any device using a supported web browser.		
11	The solution must include agent software that is deployed on all managed desktops and servers.		
12	Tool to support configuring time window for any particular software for exceptional usage purpose.		
	<b>Reporting Requirements</b>		
1	The solution shall include a web-based reporting module.		
2	Information reported shall not be more than 1 day old for devices that are active on the network.		
3	Access to reporting function shall be controlled based on rights assigned by the Administrator.		
4	The reporting module shall contain, but not be limited to, the following reports: Progress of all patches applied & patch management tracker		
4.1	Number of vulnerabilities detected by month		
4.2	Total number of computers managed and the distribution of these computers		
4.3	Top 10 most common vulnerabilities detected		
4.4	List of software installed on each agent		
4.5	list of compliant and noncompliant edpoints/servers ,		
4.6	List of total managed and unmanaged endpoints and servers		
4.7	List of missing & installed patch on endpoints and servers.		
4.8	list of endpoints and server where agent is not reachable/failed		
5	Allows console operators to create and save reports from a list of built-in default reporting templates as well as the flexibility of creating & generating custom reports.		

6	Able to generate reports on Hardware and Software inventory information.		
7	To generate customized reports on Hardware and Software inventory information.		
8	Able to generate reports on asset properties that are fetched by the agent.		
9	To create filters to include or exclude certain categories of information from the reports.		
10	To schedule report generation and share the same through Email		
11	The Tool should be able to provide/maintain report data from the implementation date		
12	The solution should be able to provide custom report in tabular format		
13	Query builder for reports/query based reports		
14	Flash reports (Flash reports are short, executive-level, summaries that provide a snapshot of a company's key performance metrics at regular time intervals. It may be a Dash board showing the periodic snapshot of key data. This report is meant for top management)		
15	Functionality to export report to .csv, .xls and .pdf format		
16	User Logon reports with login history		
17	Configuration reports should be available		
18	Patch reports should be available		
	<b>Application Control</b>		
1	Solution should block non-business applications		
2	Solution should provide need-based application-specific privileged access.		
3	The solution shall handle interim user who needs by enabling temporary application and privileged access that are automatically revoked after a set period.		
2	The solution shall grant on-demand access to unmanaged applications requested by users.		
3	The solution should be capable to blacklist the application. The blacklisted application should not install and should not run on the specific endpoints/ group of endpoints/servers.		
4	The proposed solution should have ability to uninstall any application on endpoints/servers without the need of specific software uninstaller.		
5	The tool should support Application/software Whitelisting of approved softwares based on different criteria (S/w OEM based, Software title based, Hash value based etc.) and blacklisting of softwares based on CVE score / on specified request.		
6	The tool should provide a Tracker of approved/whitelisted application for review.		
7	The tool should provide Application/software Inventory details.		
8	The tool should provide Tracker for the software that are allowed on exception basis		



	<b>Software Inventory Management</b>		
1	Able to list all software and applications, including version numbers, which are installed on the agent.		
2	Inventory changes are automatically processed at the agent and sent to the server without operator intervention.		
3	Able to list all software and applications installed for a group of computers, including the number of installations for each software and application.		
4	Able to list all services running on a particular agent.		
5	Allow console operators to edit the registry entries of selected computers via the central console.		
6	Solution should have facility to create custom queries on software inventory information retrieved by the agents.		
7	Solution should have facility to create custom actions to be performed on computers (e.g. Stopping a service)		
8	Ensure compliance: Use out-of-the-box dashboards to easily view and manage compliance status		
9	Physical tagging : For all IT asset physical tagging of assets is required as per the Tagging scheme advised by bank , Physical Tagging will be done by bank team . The software should generate the tag .		
	<b>Management of Agents</b>		
1	The solution should enable the management of all computers from a console.		
2	The Administrator shall be able to perform the basic management tasks from the console: i) Configure all agent settings centrally ii) Create Dynamic computer groups iii) Create Users with Role Based Access Control iv) Assign agents to Distribution points		
3	Setup bandwidth Throttling		
4	Perform software upgrade of agents remotely		
5	The solution should enable monitoring of the status of all agents from a console.		
6	The User Interface for Administration i.e. Console should provide flexibility to allow users to customize the console to fit their individual requirements by adding, and removing column headers/functions based on the role of the user.		
7	The solution should enable to group computers statically by selecting computers and adding to the group or dynamically based on the result of inventory properties such as e.g. Active Directory groups,Active directory OU, OS, IP range etc.		
8	Solution Agent should provide an end user Information interface that allows the user interacts with the agent for interactive actions		

9	The solution should enable administrators to hide the agent from the computer's "Add/Remove Program" .		
10	If the agent fails to communicate to the server within a specified interval, the solution shall automatically mark the agents as offline.		
11	The solution should able to assign devices group /custom group / remote offices based on the ip address to administrator		
12	The Solution should create endpoint and server profile based on their unique identifier to avoid duplicate entries.		
<b>Software Usage and License usage reporting</b>			
1	The Analysis should include the following information (but not limited to) with the ability to drill down for more detailed views: i)Publisher name ii)Software title name iii)Software title version iv)Total computers Count		
2	Web UI should allow Role Based access to allow or restrict users' privileges by their role.		
3	Web UI should have the ability to view, filter, and sort upon user input to create custom reports.		
4	Ability to view all properties & raw data gathered from the agent during the inventory process.		
5	Ability to create groups based on inventory properties like (but not limited to): i)Subnet Address ii)Operating System		
6	Ability to create License Compliance reports based on the details specified in License Contracts that were created.		
7	The product must be capable of generating license compliance reports for Windows /Linux and Other Major OS platforms available in the market.		
<b>INVENTORY</b>			
1	Software license compliance to view over-licensed and under-licensed software used in the network		
2	The Solutions must provide device network discovery and inventory of all hardware and software connected to your network, including computers, servers and non-computing network devices. The support platform must include, but not limited to Windows, Mac, Linux, Chrome OS etc. Should also Discovery VM's and its resources by integrating with Hypervisor		
3	The Solutions must provide Software IT asset management for comprehensive asset tracking and compliance reporting		
4	The Solutions should allow to import offline asset inventory		

5	The Solutions must provide the interactive Software Asset Dashboard for high-level overview of your asset usage for quick review of assets usage and maintain the licenses associated with for avoiding unnecessary renewals		
6	The Proposed Solutions should be capable of Asset allocation to single user, Asset allocation to multiple users, Asset allocation to project, Asset allocation to department, Asset allocation to location, Bulk Allocation of Assets, Asset Return & Re-Allocation process		
7	The Solutions must provide the options to manage and maintain Software compliance under software inventory		
8	The Solutions should support software catalogue which should allow or restrict software items to be considered License Compliance accordingly Bank policy		
9	The solution must be capable of proactively reporting changes to managed desktops within a few minutes of detecting change or upon executing any action deployed from the server.		
10	Assets profile need to be done on the basis on unique identifier		
11	The proposed solution should consolidate, end-to-end lifecycle management of IT hardware and software assets.		
12	The proposed solution should provide Software Asset Management Compliance Dashboards.		
13	The proposed solution should provide License Reconciliation feature like Automated reconciliation of licenses between versions based on utilization delivers a software version matrix so easily upgrade or downgrade licenses.		
14	Provide dashboards that provide a quick overview of various kinds of assets, allowing you to understand, organize, and track assets effectively.		
15	Efficiently track and manage assets through life cycle with out-of-the-box workflows. Customize rules to manage workflows based on business needs.		
16	Understand and manage assets by creating relationships between devices and service components, system element records, infrastructure, and peripheral assets.		
17	The proposed solution should provide Software Asset Management feature, but not limited to: i. Built-in smart dashboards and compliance tools ii. Vendor specific predefined license rules and metrics iii. Optimal utilization of licenses iv. Software asset management optimization v. Compliance management through dashboards and reporting		
	<b>Asset Inventory Requirements Asset Discovery</b>		
1	The solution must provide a decentralized discovery process that will not impact network traffic or security.		
2	Solution should provide a wizard to configure and schedule scans.		

3	The 'scan point' should only upload the differences from the last scan.		
4	Discovery should work without requiring agent installation (that is, agent-less discovery)		
5	Should use Industry-standard protocols such as WMI, SNM to perform discovery		
6	Proposed Tool should be able to provide accurate discovery		
7	Solution should maintain the discovery of historical data as well as up to date information and also detect the asset changes.		
	<b>Hardware Inventory Management</b>		
1	Able to retrieve hardware asset information from the systems which have the agents installed without the need of scheduling an inventory scan.		
2	Inventory changes should be automatically processed at the agent and sent to the server without operator intervention.		
3	All hardware asset information shall be recorded in the management server and some of the basic information shall include but not limited to: a.CPU speed and type b.Hard disk space c.Computer name d.Computer model e.IP address f.Operating System g.Attached peripherals h.MAC Address i.RAM		
4	Solution should allow to create custom queries on hardware asset information retrieved by the agents.		
5	Able to dynamically group computers based on the hardware asset information.		
	<b>Remote Control</b>		
1	This solution is expected to take complete desktop control of Windows desktops/servers from a central location.		
2	It shall support security-related features for taking the control of remote PCs, based on security group on active directory .		
3	The solution should support 256-bit Advanced Encryption Standard (AES) encryption protocols during remote access operations.		
4	It shall provide flexibility with respect to the type and capability of the remote control session like: i. Full control of the remote PC not only in client server mode but also over the Webii. Monitor-only-mode.		
5	It shall support locking of keyboard and mouse of the remote PC.		
6	It shall support file transfers		

7	Roles should be used to restrict the level of operations an administrator can perform. The Remote Control should offer the least the following four roles: i. Control - Take control of the remote machine; execute commands and applications (active state) ii. Monitor - View the display of the remote workstation and monitor activities (monitor state) iii. Reboot - Reboot the remote workstation iv. File transfer - lets you transfer files and directories from endpoint to endpoint		
8	The Remote Control should also be able to create target lists/groups. Lists/groups restrict administrator access to a specific group of machines, increasing security and performance.		
9	Web Browser Interface - Solution should provide a web interface with below mentioned capabilities		
10	The Remote control module should provide an authorization-based Web Interface for Administrators to facilitate Remote control using a browser. It should support all the functions i.e. Remote Control, Files Transfer, etc. through the Web Browser Interface.		
11	It should provide enhanced central logging to track session information including controller ID, target host name, session policies, and auditable events such as user acceptance, file transfer operations, session mode changes, and chat transcripts.		
12	It should provide Active Directory authentication and data synchronization.		
13	It should provide full data stream encryption for all communications and file transfers between controllers and targets.		
14	It should provide automatic session lockout due to administrative inactivity.		
15	It should terminate the remote connections if they are idle for a specific duration.		
	<b>All the installation should be done by the OEM or OEM certified Engineer</b>		
	<b>All the licenses should be perpetual in nature in the Bank name.</b>		

<b>Patch Management for s390x Platform</b>			
<b>S. N.</b>	<b>Technical Specification for Endpoint and Patch Management Solution</b>	<b>Bidder's Compliance (Yes/No)</b>	<b>Bidder's Remarks</b>
1	The solution must support Patch Management solution for patching Red Hat Enterprise Linux 8/9(RHEL 8/9) and above Operating System on IBM LinuxOne Z Systems with S390x Architecture.		

2	The solution should have centralized automated patching on the servers.		
3	The solution should have various patching policies.		
4	The solution should have test patching before proceeding for production patching i.e. patch lifecycle.		
5	The solution should be able to bifurcate of the unrelated patches for various applications needs.		
6	The solution should have custom groups for server patching.		
7	The solution should have single dashboard / console for the Patching environment.		
8	The Solution should have Monitoring and Reporting features		
9	The solution should have the REDHAT repositories.		
10	The Solution should have the Discovery and Assessment features		

<b><u>AD Management Solution</u></b>			
<b>S. N.</b>	<b>Technical Specifications for AD Management Solution</b>	<b>Bidder's Compliance (Yes/No)</b>	<b>Bidder's Remarks</b>
1	Proposed solution should be a web-based solution with SSL and session expiry and should support following functionalities:		
2	-Centralized user creation for Active Directory		
3	-Re-setting forgotten passwords		
4	Solution should have Movement of users and bulk movement from one Organizational unit to another		
5	Solution should Reset the passwords of multiple computers at once to the default initial value, and more.		
6	Solution should have Addition and removal of Admin users (makers and checkers)		
7	Solution should be Reviewing and editing available entitlements		
8	Solution should Add/remove users from groups, set primary groups of users, and more.		
9	Solution should Create multiple AD security and distribution groups, and assign various group attributes at once.		
10	Solution should Delete multiple AD groups, in bulk, at once.		
11	Solution should Bulk create and modify AD contacts and the respective attributes.		
12	Solution should Delete AD contacts individually or in bulk by importing a file containing the list of contacts to be deleted.		
13	Solution should Move AD contact objects, in bulk, between OUs.		

14	Solution should Bulk create, delete, and move OUs with just mouse clicks.		
15	Proposed solution should support multiple admin facility at distributed locations viz zones, regions with respective jurisdiction of user management. Proposed solution should have administrator available at centralized location at Central Office		
16	Proposed solution should have provision of temporary user in-activation based on feed received from PeopleSoft HRMS solution		
17	Proposed solution should be able to reconcile the users with HRMS and provide list of such additional users		
18	In proposed solution, any change in user attributes should be through HRMS feed. i.e. solution should have an option to compare relevant attributes of users like mobile no, email id etc. in AD with that of HRMS and any change in HRMS should be reflected in AD through maker and checker option		
19	Proposed solution should have provision for users as well as admins to add or modify Mobile no., e-mail address, office location etc.		
20	Proposed solution should provide tamper proof audit trails and logs of user maintenance activities that are acceptable to the court of law		
21	Proposed solution should support approval workflow mechanism with Maker and Checker facility for all administrative activities like user creation, activation, password reset, movement from one office (OU) to another, addition of attributes, changes in attributes like mobile no. & e-mail id in AD, admin delegation etc.		
22	Proposed solution should support multi-domain Active Directory Forest		
23	Proposed solution should support centralized user/ bulk users' creation from the feed of PeopleSoft HRMS or any other application		
24	Proposed solution should have attributes like user expiry on date of retirement or any other specific date during user creation. For existing users, proposed solution should have an option to feed the user expiry through bulk file upload mechanism		
25	Proposed solution should capture comments /remarks for any activity carried out by the maker and the checker		
26	Proposed solution should have built-in support for Segregation of Duties (SOD)		
27	Proposed solution should support Detective Segregation of Duties analysis		
28	Proposed solution should support Preventive Segregation of Duties analysis		
29	Proposed solution should facilitate the admins to fetch all attributes of a specific user or group of users		
30	Proposed solution should have dashboard functionality to view details of users and systems		

31	Proposed solution should have facility to restrict specific users to login within specific time frame		
32	Proposed solution should not have any limitation in terms of number of users		
33	Proposed solution should have option to set specific default password without feed while resetting password, if required		
34	Proposed Solution should serves as a centralized password manager for bulk password management, automated password reset, and actionable password reports.		
35	Proposed solution should have functionality to delegate powers to admin by super admin / two admins of the same group through maker & checker concept		
36	Proposed solution should be a part of Microsoft Active Directory (AD) domain		
37	Proposed solution should have native integration with Microsoft Active Directory		
38	Proposed solution should provide an environment to perform, test, commit or rollback all UI (user interface) customizations without impacting other users		
39	The solution should be able to create, modify, and manage the GPOs.		
40	The person creating GPOs should be only a normal user in the AD and he should not be able to approve the GPO roll out		
41	Solution must be able to audit GPO changes, verify its consistency & also compare GPO version side-by-side.		
42	Solution must have provision to revert the GPOs to the previous version.		
43	Solution should allow approval workflows so that the person creating the GPO should obtain approvals before rolling out the same		
44	Solution must have capability to test pre-production GPO clones before rolling them out.		
45	Solution should be able to lock down the GPO objects so that others are not able to edit the same while one administrator is editing it		
46	The solution should be able to compare the GPO settings for two GPOs side by side		
47	Solution should have Object protection feature for Active directory objects like Group Policy, Organizational unit etc so that even the insider threats do not gain access to the protected objects using native Active directory management tools. The tool should also be able to configure time based proactive protection/lock down for critical AD objects		
48	The solution should restrict the Default Administrators as well as other privileged users other than the ones explicitly permitted, from linking the GPOs to specific OUs and modifying any protected tier zero objects in the AD		
49	Solution should Enable or disable multiple user accounts and also specify the account expiry date		



50	Solution should Create and manage GPOs and GPO links.		
51	Solution should Create and manage users, groups, contacts, and licenses.		
52	Solution should Generate reports on users (including passwords, user logon, and account status), groups, contacts, and licenses.		
53	Solution should Configure a second authentication method (Single sign on, two factor authentication, or smart card authentication) to login to the product.		
54	Solution should Define an order of execution for management operations, with different checkpoints like request, review, approve, and execute.		
55	Solution should Create workflow requests for AD objects creation (users) and modification (users, computers, contacts, groups.)		
56	Solution should Employ full automation or controlled automation to carry out any management/administrative task such as AD cleanup, group membership management, and so on.		
57	Solution should Automate a sequence/series of tasks and also specify the intervals at which each task in the sequence should be executed.		
58	Solution should Create personalized naming formats as per Bank policies.		
59	Solution should Add/remove titles, departments, offices, and companies based on Bank needs.		
60	Solution should Configure a custom format that has to be adhered to, for generating random passwords.		
61	Solution should Set up domain-specific delete and disable policies that will be executed whenever user accounts are disabled or deleted.		
62	Proposed solution should have features of self-managed password reset using OTP through e-mail id/mobile number, which should be available in integration with Bank's existing mail and SMS gateways		
63	Proposed solution should respond to pre-defined failed attempts through relevant error		
64	Proposed solution should support reports related to access policy, request, attestation, approval, role, organization, password, resource & entitlement, user. e.g. list all users created in a specified time period. Detail should include method of user creation (manually or through trusted reconciliation), all the deleted users, list of users whose accounts are disabled, list of users whose disabled accounts are unlocked by administrators, list all existing users provisioned to a specified resource, user's resource entitlement history over user's lifecycle (reporting is key capability for getting in-detailed information)		
65	Proposed solution should have functionality to auto generate report of new users created at the end of the day and the same should be populated/mailed to respective admin/super admin.		
66	The predefined reports should be customizable		

67	The audit reports should be easily exported to various reusable file formats including PDF, HTML and XLS etc.		
68	Solution should have the capability to alert if an unauthorized attempt is made for configuration changes in AD.		
69	Proposed solution should have availability of time stamped reports like user details with date of creation, user movement, activities carried out by specific maker or checker, list of users for which password reset done etc. for a particular period		
70	Solution must have Real-time auditing & alerting capabilities		
71	Solution should have capability to audit account lockouts.		
72	Proposed solution should capture IP address of the system while logging-in to the solution or while initiating any request through the solution, which may not require to log-in to the solution		
73	Proposed solution should throw warning message and reports for abnormal activities like password reset of around 50 users of one Region, password reset of one user twice a day, User creation with identical name, user movement from one OU to other twice a day, any activity done beyond normal working hours (i.e, other than 10:00 AM to 06:00 PM)		
74	The solution should provide live dashboard with the changes in the Active directory with Who is making the change , what is the change, from where the change is made from including the time of the event		
75	The solution should provide live updates for the events like failed logon attempts, successful logons, user creation etc		
76	Administrator should be able to configure alerts on email for specific event criteria with capability to mention thresholds for those events		
77	Solution should Demonstrate product compliance with various regulatory compliance mandates		
78	View the list of all actions (creation, deletion, and modification) performed		
79	View the logon details of admin, along with details such as their logon status, and authentication methods for all their logons.		
80	Solution should Facilitate backup of entire Active Directory forest data		
81	The solution should be able to compare between two backups and between backed up data with live AD data		
82	Recovery solution support single user and single attribute recovery without bringing the production AD offline		
83	Solution must be able to restore AD object, including users, groups, computers, organizational units, sites, subnets, configuration and Group Policy Objects (GPOs)		
84	Solution should provide password based encryption to protect the backed up data		
85	Solution should have web interface to Delegate data restore tasks to specific users.		
86	Proposed solution should integrate with any SOC and Application Change Control solution		

87	Solution should have option to deploy and uninstall the agent remotely.		
88	The solution should be able to generate reports on the below		
89	1) Critical group membership changes		
90	2) Nested group changes		
91	3) computers added / disabled / moved / renamed		
92	4) OUs added/deleted/renamed etc		
93	5) Users added/ disabled / deleted / renamed in last 30 days		
94	6) Users unlocked in last 30 days		
95	7) Users expiration date changed in last 30 days		
96	8) User profile changes in last 30 days		
97	Proposed solution should have ability to identify rogue and orphaned accounts		
98	Should have option to archive and purge older events.		
99	Should have web-based access interface with dashboard reporting for compliance.		
100	Solution should Fetch general computer reports and account status reports of all computers in your AD.		
101	Should Obtain OU-related information such as users/computers-only OUs, recently created/modified OUs, and more.		
102	Generate reports related to AD objects accessibility, servers, subnets, search permissions, and more.		
103	Generate reports based on LDAP queries and custom attributes of AD objects.		
104	All the reports provided by the proposed solution should be in HTML, CSV, TXT and PDF formats		
105	Proposed solution should not reveal any password at any point of time		
106	Proposed solution should be able to be hosted on virtual machines (Vmware & Nutanix) and solution should be installed on latest Operating System.		
107	Proposed solution should have a DRC set-up which should be synched with DC as per RTO and RPO acceptable to the Bank		
108	Proposed solution should function in High Availability (HA) mode		
109	Proposed solution should provide scheduled back-up mechanism		
110	Proposed solution should support IPV4 and IPV6		
111	Proposed solution should have redundancy and failover capabilities built-in which Bidder needs to specify separately		
112	Proposed solution should have proper error message handling i.e. solution should give proper error message.		
113	Proposed solution should support integration with Bank's existing biometric solution		
114	Should be able to audit the service principle name changes of users, irregular domain controller registration activity and changes to SID History of user and group objects		

115	Solution should be Agent-based to eliminate need native event logs		
116	Proposed solution should trigger email alert for password expiry of specific application users.		
117	Proposed solution should trigger email alert for account expiry of specific application users.		
118	Proposed solution should have provision to schedule reports periodically like all active users, all disabled users, all active computers and all disabled computers etc.		
119	Proposed solution should have provision to disable inactive systems in AD.		
120	Proposed solution should have provision to generate report for specific AD group member		
121	Proposed solution should have provision to add / remove bulk users in specific AD group by taking input from csv, text or excel file.		
122	Proposed solution should have provision to generate report for above point		
123	<b>The bidder has to install and commission Microsoft ADFS (Active Directory Federation Services) solution in the Bank. Bidder has to provision Microsoft Services for installation of the same.</b>		
	<b>All the installation should be done by the OEM or OEM certified Engineer</b>		
	<b>All the licenses should be perpetual in nature in the Bank name.</b>		

<b><u>SFTP</u></b>			
<b>S. N.</b>	<b>Technical Specifications for SFTP solution</b>	<b>Bidder's Compliance (Yes/No)</b>	<b>Bidder's Remarks</b>
<b>1</b>	<b>Technical Specification</b>		
1.1	Proposed solution should be a web-based solution with SSL (TLS 1.2 , 1.3, 2048bit) and session expiry		
1.2	Proposed solution should have automation available to pull and push files to different location in SFTP server. It should be based on condition too.		
1.3	Proposed solution should support automatic file transfer from one SFTP to another SFTP server, once public key is made available to other third party SFTP server. File transfer should not ask credential again while moving files.		
1.4	Proposed solution should support Active Directory authentication		
1.5	Proposed solution should integrate with any SOC, DLP, PIM and Application Change Control solution		
1.6	Proposed solution should assign virtual folder to two user, so the root folder would be available for both the users		

1.7	Proposed solution should support Edge browser and above; should run on any Windows operating System Viz Windows 10, Windows 11, etc. and should support all versions of Firefox and Google Chrome		
1.8	Proposed solution should capture IP address of the system while logging in to the solution or while initiating any request through the solution		
1.9	Proposed solution should provide tamper proof audit trails and logs of any changes/actions made on server and should be available in the format presentable in court of law		
2	In the proposed solution, Admin users should act only upon the users under their jurisdiction		
2.1	Proposed solution should have availability of time stamped reports like File creation, Transferred to source/destination location, User changes, Users actions and modification, Permission which are allowed/disallowed in folders		
2.2	Proposed solution should provide all reports in HTML, CSV, TXT and PDF formats		
2.3	Proposed solution should facilitate the admins to fetch all attributes of a specific user or group of users		
2.4	Proposed solution should have dashboard functionality to view details of File transfers / User actions / Usage / Files type / Error in any Log or Transfer		
2.5	Proposed solution should have facility to restrict specific users/IP to login within specific time frame, white-listing and black-listing of IP should be available as well		
2.6	Proposed solution should support authentication using OTP from email Id/mobile number, which would be available in integration with Bank's existing mail and SMS gateways		
2.7	Proposed solution should not reveal any password at any point of time		
2.8	Proposed solution should support integration with Bank's existing biometric solution/2 factor authentication		
3	Proposed solution should function with 16 Kbps of bandwidth availability since Bank's VSAT branches are having minimal network bandwidth		
3.1	Proposed solution should function smoothly with around 50 concurrent sessions		
3.2	Proposed solution should be able to be hosted on virtual machines (Vmware & Nutanix) and should be installed on latest Operating System		
3.3	Proposed solution should have a DRC setup which should be synched with DC as per RTO and RPO acceptable to the Bank		
3.4	Proposed solution should provide scheduled backup mechanism		
3.5	Proposed solution should support IPV4 and IPV6		
3.6	Proposed solution should have built-in redundancy and failover capabilities which Bidder needs to specify separately. Proposed solution should also need High Availability and fault tolerance configure at application level.		

3.7	In case proposed solution has a database then it should be a Oracle database. If any other database than Oracle is proposed, Bidder should provide database license cost as well as OEM support for 5 years in the Bill of Material		
3.8	Proposed solution should have proper error message handling i.e solution should give proper error message, alert via mail or dashboard		
4	Proposed solution should have functionality to send report automatically to specific party at specific time		
4.1	Any additional hardware/software for successful implementation of the solution need to be provided by the Bidder		
4.2	Proposed solution should define threshold per user, regards to disk usage / disk quota, Folder level quota (Storage), should be applied uniformly across all users irrespective of no of users part of that folder.		
5	Configuration level changes made on particular site should be applied to all users part of that site and same should be available in report form whenever changes are made.		
6	For disable users in sftp application , archival process should be enabled to migrate disabled users.		

<b><u>Load Balancer</u></b>			
<b>S. N.</b>	<b>Technical Specifications for Server Load Balancer for Web Layer - 2 -DC &amp; 2- DRC</b>	<b>Bidder's Compliance (Yes/No)</b>	<b>Bidder's Remarks</b>
<b>1</b>	<b>Technical Specification</b>		
1.1	The proposed solution should support Advance Appliance Clustering		
1.2	The proposed solution should have API to integrate with any leading SDN & Cloud Orchestrators like Cisco ACI, VmWare NSX, OpenStack, CloudStack.		
<b>2</b>	<b>Hardware Specifications</b>		
2.1	The Proposed Solution must be Hardware Appliance based.		
2.2	The proposed solution should have minimum 16x10G/25G multi mode fibre ports from day1. The SFP supplied should be from the same OEM .		
2.3	The Proposed Solution must have redundant power supply.		
2.4	The Proposed Solution should be delivered using Single Tenant.		
2.5	The proposed appliance should support minimum 80 million L4 concurrent connections.		
2.6	The proposed appliance should support minimum 40Gbps encryption throughput		
<b>3</b>	<b>Traffic Management</b>		
3.1	The Proposed Solution should support Server Load balancing.		

3.2	Algorithms: Round Robin, Least Packets, Least Bandwidth, Least Connections, Response Time, Hashing (URL, Domain, Source IP, Destination IP, and CustomID), SNMP-provided metric, Server Application State Protocol (SASP)		
3.3	This should also support Priority Queuing, Link Load Balancing, Dynamic caching		
3.4	Protocols supported: TCP, UDP, FTP, HTTP, HTTPS, DNS (TCP and UDP), SIP (over UDP), RTSP, RADIUS, DIAMETER, SQL, RDP, IS-IS, SMPP		
3.5	The Proposed Solution should support minimum L7 60 Gbps throughput		
3.6	The Proposed Solution must have performing load balancing for Layers 4 through 7 of the Open Systems Interface (OSI) reference model with support to the IP, TCP and UDP protocols.		
3.7	The Proposed Solution must have performing load balancing for Layers 4 through 7 based on source/destination IP		
3.8	The Proposed Solution must have performing load balancing for Layers 4 through 7 based on application content		
3.9	The Proposed Solution should do load balancing based on weights defined on Real Webservers.		
3.10	The Proposed Solution must do load balancing based on SNMP, TCP, Bandwidth, Response time, health of the Server.		
3.11	The Proposed Solution must support load balancing based on cyclic (round-robin)		
3.12	The Proposed Solution must have load balancing based on least connections, Hashing, Persistency based ( Cookie, Client IP, SSL ID etc.)		
3.13	The Proposed Solution must have virtual servers that can listen on UDP and TCP ports		
3.14	The Proposed Solution must have the ability to enable and disables server gracefully and hard shutdown.		
3.15	The Proposed Solution must have HTTP 2.0 gateway.		
3.16	The proposed solution must have L7 HT TP Requests/Sec 2.4M		
<b>4</b>	<b>Persistency</b>		
4.1	The Proposed Solution must have session persistency based on Layer 3 and Layer 4.		
4.2	The Proposed Solution must be able to make persistency decisions based cookies ( Insert/passive)		
4.3	The Proposed Solution must have option to do script based Persistence		
<b>5</b>	<b>Health Monitoring</b>		
5.1	The Proposed Solution must have the ability configure TCP and UDP health check for real web servers.		
5.2	The Proposed Solution must have health monitoring that mark web servers unavailable based on retrieval of a Web page for unique content.		

5.3	The Proposed Solution must have the ability to specify a minimum number of health check to mark a Real Server as being available		
5.4	The Proposed Solution must have multiple health checks per IP and per port		
5.5	The Proposed Solution must have the ability to specify the number of retries for each health check before marking a Real Server unavailable.		
5.6	The Proposed Solution must have support creating application specify custom health check using scripts.		
<b>6</b>	<b>SSL Acceleration and Central</b>		
6.1	The Proposed Solution must have SSL offload - the ability to manage client side SSL traffic by terminating incoming SSL connections and sending the request to the server in clear text		
6.2	The Proposed Solution Should support end to end SSL.		
6.3	The Proposed Solution Should support minimum 60K SSL Transactions per second for 2048 bit key (1 TPS == 1 CPS).		
6.4	The Proposed Solution must have hardware based SSL acceleration		
6.5	The Proposed Solution should support 1024, 2048 and 4096 bit key for SSL offloading		
<b>7</b>	<b>TCP Multiplexing</b>		
7.1	The Proposed Solution must have TCP Multiplexing		
7.2	System support HTTP connection pooling		
<b>8</b>	<b>HTTP Compression</b>		
8.1	The Proposed Solution must have HTTP compression		
8.2	The Proposed Solution Should support minimum 35 Gbps of compression throughput		
8.3	The Proposed Solution should Selective compression to avoid know compression problems in commonly used browsers		
<b>9</b>	<b>Mode of integration, IP Addressing (IPv4 and IPv6) and Routing features</b>		
9.1	The Proposed Solution must have one-arm , two-arm mode deployment		
9.2	The Proposed Solution must have direct server return mode		
9.3	The Proposed Solution Should support IPv4 addressing		
9.4	The Proposed Solution Should support IPv6 addressing		
9.5	The Proposed Solution Should support IPv6 client and IPv4 servers		
9.6	The Proposed Solution Should support IPv4 client and IPv6 servers		
9.7	The Proposed Solution Should support routing protocols RIP, OSPF and BGP.		
<b>10</b>	<b>Global Server Load Balancing</b>		
10.1	The Proposed Solution must have Global Server Load Balancing supported on the same appliance		



10.2	The Proposed Solution must have performing load balancing across multiple geographical sites for transparent failover, complete disaster recovery among sites and optimal service delivery , Single application failure etc.		
10.3	The Proposed Solution must have global response time optimization in real-time through advanced load and proximity measurements		
10.4	The Proposed Solution must have providing failover capability between data centers in active-active or active-backup modes		
10.5	The Proposed Solution must have global redirection based on DNS		
10.6	The Proposed Solution DNSSEC functionality		
<b>11</b>	<b>Performance Monitoring</b>		
11.1	The Proposed Solution Should be able to monitor TCP , HTTP Based applications.		
11.2	The Proposed Solution Should track Page Load Time (Tracks how long it takes an application user to get a complete response from the application, including network latency and completed page processing ).		
11.3	The Proposed Solution Should be Identifying the root cause of slow performance issues		
11.4	The Proposed Solution Should be able to collect statistics for Client IP address (Saves the IP address where the request originated).		
11.5	The Proposed Solution Should be able to collect statistics for URL.		
11.6	The Proposed Solution should Display the usage of web applications across different geographical locations on a map		
<b>12</b>	<b>Clustering Redundancy</b>		
12.1	Ability to Scale beyond the pair ( Active - Active -N).		
12.2	Automatic syncing of common config across the nodes		
12.3	Disruptive failover events - both at the device and the service (application) level.		
12.4	Scaling Out a VIP across the cluster (Spanned Virtual Server)		
12.5	Traffic Distribution ( System should support Equal Cost Multiple Path (ECMP -> Dynamic Protocol OSPF , BGP )) or Cluster link aggregation mechanism )		
<b>13</b>	<b>Service and Support</b>		
13.1	The devices and software should be supported by the OEM on a 24x7 basis through a global Technical Assistance Center (TAC). The support should include 4 Hrs Advance Replacement (Delivery within 4 hours after authorization of replacement).The support should be provided direct from OEM and not through any intermediate third-party.		
<b>14</b>	<b>Management Console</b>		
14.1	Web-based UI: HTTPS/SSL secured GUI accessible via a browser		
14.2	CLI (Command Line Interface): For advanced configuration and troubleshooting		

14.3	API Support: RESTful API or SOAP for automation and integration with other management systems		
14.4	Real-time Dashboard: Provides graphical insights into traffic, health checks, and system metrics		
14.5	Logging and Reporting: Generates detailed logs of requests, errors, and performance metrics		
14.6	Alerts and Notifications: Configurable alerts for health check failures, high latency, or unusual traffic		
14.7	Historical Data: Stores analytics data for trend analysis and troubleshooting		
14.8	Access Control: Role-based access control (RBAC) for administrative users		
14.9	IP Whitelisting/Blacklisting: For securing access to the console		
14.10	Audit Logs: Track configuration changes and administrative actions		
14.11	Backup and Restore: Configuration backup and restore options		
14.12	Firmware Management: Updates and patches via the console		
14.13	Resource Monitoring: CPU, memory, and disk usage monitoring		

<b><u>Antivirus Solution</u></b>			
<b>S. N.</b>	<b>Technical Specifications for Antivirus</b>	<b>Bidder's Compliance (Yes/No)</b>	<b>Bidder's Remarks</b>
1	The proposed endpoint security solution should be using a blend of advanced threat protection & detection techniques to eliminate threats entering in to Bank's Network and is delivered via an architecture that uses endpoint resources more effectively and ultimately perform considering CPU and network utilization.		
2	The proposed solution should protect and secure the endpoints & desktops running OS platforms Windows 10, 11 and latest version		
3	The proposed solution must provide centralized management console for consistent security management, complete visibility of all the end-points, configuration management and reporting functionality.		
4	The proposed solution should be able to defends endpoints against malware, Trojans, worms, spyware, addware, ransomware, and adapts to protect against new unknown variants and advanced threats like crypto malware and fileless malware in order to detect and respond to the ever-growing variety of advanced malware threats, including fileless attacks and ransomware.		
5	The proposed solution must have multiple techniques to address known,unknown,unpatched threats with pattern/signature based, behavior monitoring, highly-		

	accurate machine learning - pre-execution and runtime, application control		
6	The proposed solution must have enhanced tamper protection that guards against unauthorized access and attacks, protecting users from viruses that attempt to disable configuration changes / uninstall by unauthorized personnel and disable security measures.		
7	The EPP solution should be on-premise solution.		
<b>Preventive Capabilities and Controls</b>			
8	The proposed solution should have prevention capabilities:		
i	• Antimalware with signature/Pattern based detection		
ii	• Ransomware protection		
iii	• Machine learning - pre-execution and runtime		
iv	• Browser exploit protection		
v	• Behavior monitoring		
vi	• Injection protection		
vii	• Script protection		
viii	• Anti-exploit		
ix	• C&C communication prevention		
x	• Application control		
xi	• File less malware prevention		
xii	• File/web reputation		
<b>Anti-Malware</b>			
9	The proposed solution must offer comprehensive security by protecting Systems from viruses, rootkits, trojans, worms, hackers, joke programs, ransomware and network viruses, plus spyware, grayware and mixed threat attacks.		
10	The proposed solution must support various scan type options to clean dormant malwares - Real time scan, Manual scan, scheduled Scan[daily/weekly/monthly] and on-demand Scan and provide options to be able to add files, folders or extensions to an 'exclude' list so that they are not scanned on access.		
11	The proposed solution must be configurable able to scan these file extensions but not limited to: .ACCDB,.ACE,.AMG,.ARJ,.BAT,.BIN,.BOO,.BOX,.BZ2,.CAB,.CDR,.CDT,.CHM,.CLA,.CLASS,.COM,.CPT,.CSC,.DLL,.DOC,.DOCM,.DOCX,.DOT,.DOTM,.DOTX,.DRV,.DVB,.DWG,.DWT,.EML,.EPOC,.EXE,.GMS,.GZ,.HLP,.HTA,.HTM,.HTML,.HTT,.INI,.JAR,.JPEG,.JPG,.JS,.JSE,.JTD,.JTT,.LNK,.LZH,.MDB,.MPD,.MPP,.MPT,.MSG,.MSI,.MSO,.MST,.NWS,.OBD,.OCX,.OFT,.OVL,.PDF,.PHP,.PIF,.PL,.PM,.POT,.POTM,.POTX,.PPAM,.PPS,.PPSM,.PPSX,.PPT,.PPTM,.PPTX,.PRC,.QPW,.RAR,.REG,.RTF,.SCR,.SHS,.SHW,.SIS,.SIT,.SWF,.SYS,.TAR,.VBE,.VBS,.VSD,.VSS,.VST,.VXD,.WMF,.WML,.WPD,.WPT,.WSF,.XLA,.XLAM,.XLS,.XLSB,.XLSM,.XLSX,.XLT,.XLTM,.XLTX,.XML,.Z,.ZIP		

12	The proposed solution should be able to automatically scan the external USB storage once it is plugged in to provide real time protection against threats		
13	The proposed solution must support customizable actions for various types of threats : Clean,Delete,Deny access, Quarantine & Pass		
14	The proposed solution must include capabilities for detecting and removing rootkits, provide Real-time spyware/grayware scanning for file system to prevent or stop spyware execution		
15	The proposed solution must scan nested compressed files (specify up to a level of 5 layers) for malwares, viruses, spywares etc.		
16	The proposed solution should scan only those file types which are potential virus carriers (based on true file type) with option of adding program to trusted list for excluding process, if required.		
17	The proposed solution should support clean up services whenever a probable threat like virus/malware is detected		
<b>Highly Accurate Machine Learning</b>			
18	The solution has highly accurate machine learning technology which provides multi-layer protection for pre-execution and on execution (runtime) of malware to address unknown security threats found in suspicious file/process.		
19	Machine learning must have Pre-execution intelligence of extracting file features and run-time analysis of file/process behavior to identify threats.		
20	Machine learning module should be able to extract multiple features from file for ex: who,when,where info, import table,header,opcode,packer existence etc. and compare it with machine learning model and predict the maliciousness of the file.		
<b>Behavior Monitoring</b>			
21	The proposed solution must have behavior monitoring module to constantly monitor endpoints for unusual modifications to the operating systems or on installed software's to provide additional threat protection from programs that exhibit malicious behavior.		
22	Behavior monitoring must have program inspection to detect and block compromised executable files and should monitor for newly encountered program downloaded from various channels like web/email/removable media.		
23	Behavior monitoring must have an Indicator of Attacks (IOA) based Prevention like:		
i	• Host file modification		
ii	• New service		
iii	• Process modifications		
iv	• Duplicated system file		
v	• Malicious PowerShell		
vi	• Credential access		

24	Behavior monitoring must have Anti-exploit module to terminate the program exhibiting abnormal behavior associated with exploit attacks. Solution must be able to detect multiple exploit techniques like memory corruption, logic flaw, malicious code injection/execution.		
25	Anti-exploit engine must support various exploit prevention techniques but not limited to Force ASLR, Null page, Heapspray.		
26	Behavior monitoring must have multiple action parameters such as allow, block, deny.		
27	Solution must support Browser Exploit Prevention - scan browsers for exploit/ script/ scan webpage and Block.		
28	The proposed solution must have an option to trust the process and exclude from the engine.		
<b>Ransomware protection</b>			
29	The proposed solution must provide a protection mechanism against ransomware in the event of a machine becoming compromised and should have feature with documents to be protected from unauthorized encryption or modification.		
30	The proposed solution must block all the processes commonly associated with ransomware and should have program inspection to monitor processes and perform api hooking to identify if program is behaving abnormally.		
31	Ransomware protection must not be limited to specific ransomware behavior/variants .		
32	The proposed solution should have capability to submit suspicious files to sandboxing for further analysis		
33	Solution should have the capability for sandbox. Solution should support Sandboxing components deployment in Bank premise only.		
<b>Web Reputation</b>			
34	The proposed solution must support adding whitelisting and Black listing of Url's/Domain.		
35	The proposed solution must be able to identify communication over HTTP/HTTPS protocols and commonly used HTTP ports.		
36	The proposed solution must be able to detect/prevention communications to Global C&C's and Allow administrators to create user defined list also.		
37	The proposed solution must support malware network fingerprinting mechanism to detect unique malware family signatures within network packets and just not rely on ip addresses/domains.		
38	The proposed solution must have damage cleanup services after detecting Command & Control communication.		
<b>Host Intrusion Prevention System - Vulnerability Protection</b>			
39	HIPS should have deep packet inspection capability to identify content that may harm the application layer, Filters		

	forbidden network traffic and ensures allowed traffic through stateful inspection.		
40	The proposed solution should have option to configure the engine mode - Prevent		
41	The proposed solution should deliver the most-timely vulnerability protection in the industry across a variety of endpoints		
<b>Host based Firewall</b>			
42	The proposed solution must support host based firewall with stateful inspection, option to create rules on the basis of Source/Destination/Port/Protocol/Application to provide stateful inspection and high performance network virus scanning		
43	The proposed solution should organize and customize methods for protecting endpoints by creating custom policies and profiles		
<b>Application Control</b>			
44	The proposed solution must have an Application Control module to enhance defenses against malware and targeted attacks by preventing unknown and unwanted applications from executing on corporate endpoints with a combination of flexible, dynamic policies, whitelisting/blacklisting and Lock down capabilities		
45	The proposed solution provides a capable allow or deny the functionality that is able to manage known and unknown applications, file types, and executables.		
46	It should Prevent potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files).		
47	The proposed solution should provide global and local real-time threat intelligence based on good file reputation data correlated across a global network. The proposed solution must have an option of importing application list to the management console		
48	The proposed solution should integrate with AD for enforcing user-based policies.		
49	The proposed solution must support adding application criteria on the basis of path,hash,certificate/Digital signature, OEM provided safe application service with allow or block actions.		
50	The proposed solution must support importing inventory of hashes to define a Application control criteria.		
51	Solution should support automatic intelligence of applications and versions for Productivity tools like Adobe, etc. (admin need not find all dll/sha/path himself)		
52	The proposed solution must support system lockdown to harden end-user systems by preventing new applications from being installed and executed apart from the inventory found during policy installation.		

<b>Device Control</b>			
53	The proposed solution must support Device control - Whitelisting/Blacklisting of devices.		
54	The proposed solution must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The Devices that are able to be restricted must include the following:		
	- USB Storage Drives (Also able to disable autorun)		
	- CD-ROM		
	- Floppy Disk		
	- Network Drives		
55	The proposed solution must support Allow/Block Actions for the supported devices.		
56	The proposed solution must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, Com/LPT , Imaging Devices, Wireless Nic, Infrared devices		
57	The proposed solution must support various permission - Full Access, Read only, Modify		
58	The proposed solution should provide option to whitelist USB devices based on device model and serial ID.		
<b>Centralized Management console and Visibility</b>			
59	The proposed solution must provide a centralized web based management console with secure browser access using SSL based encryption		
60	The management console should be able to integrate with Active Directory		
61	The centralized security management console should ensure consistent security management and complete visibility and reporting across multiple layers of interconnected security.		
62	The proposed solution provides a secure web-based management console that gives administrators access to all endpoints and coordinates the automatic deployment of security policies, pattern files, and software updates on every agent.		
63	The centralized management console should be capable of - deploying regular signature files, - scan engines, -emergency release of signature files, - patches, hot fixes - New product versions for all managed products		
64	The management console should have an option of creating users with different user roles for managing the solution or support role-based access control		
65	The management console should support API integration to integrate programmatically with another security tools.		
66	The proposed solution must support reporting option with One time/Scheduled/Custom in CSV/PDF/RTF formats.		
<b>PSP support</b>			
67	The proposed OEM vendor should provide highest level of support and should assign a designated Technical Account		

	Manager( TAM) on OEM payroll for addressing all critical issues whenever a support ticket is raised		
68	Bank should have 24*7 access to TAM and online submission portal for product and malware related issues with priority case handling.		
69	The OEM TAM should conduct half yearly health check for the deployed solution . The health check should cover detailed configuration audit , findings and recommendations of the deployed solution.		
70	The OEM TAM should conduct onsite meetings with the concerned Bank officials to present the findings of the health check and suggest required corrective actions.		
71	The OEM TAM should provide monthly status reports for the support cases raised for that month with concerned Bank officials.		
72	The OEM TAM should proactively provide security advisories, product version release etc with the concerned Bank officials and should also extend all required support to the partner in implementing new product releases.		
<b>Alerts and Reports</b>			
73	Solution Should have the capability to generate User based Alerts and Reports in case of following events		
a	Virus outbreak alert		
b	Special virus alert		
c	Virus found- first and second actions unsuccessful		
d	Virus found - First action successful		
e	Virus found - Second action successful		
f	Network virus alert		
g	Suspicious vulnerability attack detected		
h	Virus detection reports		
	i. Viruses detected		
	ii. Most commonly detected viruses (10,25,50,100)		
i	Antivirus client information reports		
	i. Detailed		
	ii. Basic summary		
j	Comparative Reports		
	i. Grouped by (Day, Week, Month)		
	ii. RANSOMWARE (Day, Week, Month)		
k	Antivirus server deployment reports		
	i. Detailed summary		
	ii. Basic Summary		
	iii. Detailed Failure rate Summary		
l	Network Virus reports		
	i. Policy Violation report: policy violations, grouped by (Day, Week, Month)		
	ii. Service violation report: Service violations, Grouped by (Day, Week, Month)		



	iii. Most common clients in violation: clients with the most violations, (10, 25, 50, 100)		
74	Signature/remediation for all new malware must be deployed across all endpoints from the central management server's setup		
75	Bidder to provide the 24*7*365 support for Implementation, Integration, Maintenance, Administration, Onsite-Support and Licenses for Centralized Endpoint protection platform (EPP)		
76	The solution should have a Report Scheduler to auto generate and distribute relevant periodic pre-defined reports to asset owner/ SPOC of departments.		
77	The scope of the project also includes training & handholding to the designated staff of the Bank.		
78	Implementation documents related to configuration, migration, and customization including other documentation such as Operations & administration manual, Standard Operating Procedure (SOP) for various modules and roles/responsibilities.		
79	The Bidder shall provide hardware sizing of the solution utilization including memory, CPU, Hard disk space & OS License (on-premises components) to the Bank		
80	The bidder should update and maintain the solution and ensure that the update and upgrades of all the components are implemented in a timely manner		
81	The bidder should also ensure that the latest versions recommended by OEM of all the components in the solution are configured in the production at any point of time during the contract period		
82	The delivered solution should ensure scalability as per Bank's requirements and ensure immediate response to the end users.		
83	Provide updates and upgrades of the product during the entire contract period, at no additional cost to the Bank.		
84	The solution must be able to detect/block/quarantine/clean the files/IT-threats for the hashes and IOC/IOA released by OEM		
85	The proposed solution should be integrated with the Bank's current security and IT operation systems like SOC, AD, email and SIEM (& SOAR)		
86	The proposed solution should schedule reports as per Bank's Policy		
87	The propose solution should provide reports such as Executive Summary, Virus Detection report, Suspicious Object detection report, Spyware/Grayware detection report, Machine Learning Detection & Top Endpoints with threats		

<b>COMMERCIAL BILL OF MATERIAL</b>	
<b>Instructions</b>	
<b>S.N.</b>	<b>Guidelines</b>
<b>I</b>	<b>Summary of Total Cost</b>
1	The bidder is expected to quote the costs for all items required for fully complying with the requirements of the RFP and the corrigendum in the respective sections of the price bid. The prices for the respective sections would be deemed to include all components required to successfully utilise the solution.
2	CBI is not responsible for any arithmetic errors in the commercial bid details sheet committed by the bidders. All formulas & arithmetical calculations will be Vendor's responsibility.
3	The bidder is expected to specify the type of licences along with the details with respect to quantity, rate, etc., wherever applicable.
4	In case the bidder includes/combines any line item as part of any other line item in the commercial bid, then this has to be clearly mentioned in the description indicating the line item which contains the combination
5	The bidder has to quote for each line item. If any line item is part of the solution proposed in the RFP response, it has to be referenced. If it is not applicable, then the Bidder has to mention Not Applicable (NA).
6	The Bidder may insert additional line items as applicable based on the solution offered in the respective tabs
7	<b>The Bidders should quote as per the format of Bill of Material ONLY and a masked replica of the Bill of Material should be enclosed in the technical bid.</b>
8	Bidder is required to cover component by component licensing details for each of the software components proposed to CBI
9	<b>The <u>masked</u> Bill of Materials which would be submitted as part of the Technical Bill of Material should contain "XX" for ALL the corresponding commercial values that will be present in the unmasked Bill of Material that will be part of the Commercial submission.</b>
10	All amounts in the Bill of Material should be in INR
11	The Bidder should to the extent possible stick to the same structure of the Bill of Material. Hence, the bidder is not expected to delete necessary rows.
12	All the prices quoted by the bidder shall be inclusive of taxes
13	Any additional number of items (software, hardware) and services to be procured by CBI in future shall be on pro-rata basis on the rates provided in the Bill of Material.
14	If the bidder has not quoted for any line item mentioned in the Bill of Material, it will deemed considered that bidder has factored the cost for the item in the Bill of Material and No Additional charges will be paid other than the one mentioned in the Bill of Material .
15	<b>The Total cost of Ownership of this tender will be the Grand Total - TCO quoted by the Bidder of the Summary Sheet of Annexure-2 Commercial Bill of Material.</b>
<b>II / III</b>	<b>Hardware and Software</b>
1	The bidder has to quote for each line item. If any line item is part of the solution proposed in the RFP response, it has to be referenced. If it is not applicable, then the Bidder has to mention Not Applicable (NA).

2	The Bidder can insert additional line items as applicable based on the solution offered in the various tabs
3	The hardware and software type , model and detailed configuration has to be clearly described in the Description column
4	The Bidder shall provide the maintenance (Warranty & AMC/ATS) for entire contract period.
4	The bidder is required to supply implement and provide warranty & AMC/ATS of the hardware & associated software required for the solution for the tenure of the contract
<b>IV</b>	<b>Installation, Implementation &amp; Migration</b>
1	Bidder shall comply to the Installation & commissioning, implementation and Migration scope provided in the RFP
2	Bidder should quote for end to end Installation & commissioning, implementation and Migration scope as mentioned in the RFP
3	Activities and functions to be undertaken for installation and implementation of the licensed software should be as per the RFP.
<b>V</b>	<b>AMC &amp; ATS</b>
1	Bidder is expected to provide a detailed break up of all products and services that are under the scope as part of the technical bid, in the technical bill of materials i.e. the above format is expected to be replicated for each item to be covered under the scope of facilities management.
3	The AMC, ATS costs for Production DC & DR have to be quoted separately
4	If required, the Bidder has to create additional line items in this section.
<b>VI</b>	<b>Training</b>
1	The rates provided by the bidders should be applicable for any additional training that CBI may require throughout the tenure of the contract (on pro-rate basis).

### **Summary**

S. N.	Item Description	Year 1	Year 2	Year 3	Year 4	Year 5	Total Amount for 5 years (in INR)	GST	Grand Total
		<b>Cost in in INR</b>							
1	Software Cost	xx					xx	xx	xx
2	Software Implementation Cost	xx					xx	xx	xx
3	Software ATS		xx	xx	xx	xx	xx	xx	xx
4	Hardware Cost	xx					xx	xx	xx
5	Hardware Installation Cost	xx					xx	xx	xx
6	Hardware AMC				xx	xx	xx	xx	xx
7	FMS	xx	xx	xx	xx	xx	xx	xx	xx
	<b>Grand Total - TCO</b>								<b>XX</b>

**\*\*All the prices quoted by the bidder shall be inclusive of taxes**  
**All cost should flow from the respective tabs of this sheet**  
**Refer to individual sheet for timelines / Year-Wise Cost**

**Total Cost of Ownership in Words:**

## Software Cost

Software Cost				YEAR 1				
S. N.	Make /Model	Details of the proposed System Software along with Version details	License Type	Quantity (X)	Rate (INR) (Y)	Total Amount (INR) (X x Y)	GST	Grand Total
	<b>Data Centre Hardware (DC)</b>							
<b>Server Software /ATS</b>								
1	ACTIVE DIRECTORY MANAGEMENT SOLUTION			50000	XX	XX	XX	XX
2	PATCH AND ENDPOINT MANAGEMENT SOLUTION			45000	XX	XX	XX	XX
3	PATCHING OF RED HAT ENTERPRISE LINUX 8/9(RHEL 8/9) OPERATING SYSTEM ON IBM LINUXONE Z SYSTEMS WITH S390X ARCHITECTURE			800	XX	XX	XX	XX
4	Red Hat VDC LICENSES Standard			10	XX	XX	XX	XX
5	SFTP for DC and DRC with replication			XX	XX	XX	XX	XX
6	Antivirus			2500	XX	XX	XX	XX
	Other (Please Specify)			XX	XX	XX	XX	XX
	<b>Total - A</b>			XX	XX	XX	XX	<b>XX</b>
<b>Note: Price to be quoted in Year 1 only Licenses are for DC and DRC</b>								

### **Software Implementation**

	Software Implementation Cost				
S.N.	Make /Model	Quantity	Total Amount (INR)	GST	Grand Total
1	ACTIVE DIRECTORY MANAGEMENT SOLUTION	50000	XX	XX	XX
2	PATCH AND ENDPOINT MANAGEMENT SOLUTION	45000	XX	XX	XX
3	Red Hat VDC LICENSES Standard	10	XX	XX	XX
4	PATCHING OF RED HAT ENTERPRISE LINUX 8/9(RHEL 8/9) OPERATING SYSTEM ON IBM LINUXONE Z SYSTEMS WITH S390X ARCHITECTURE	800	XX	XX	XX
5	SFTP for DC and DRC with replication	xx	xx	xx	xx
6	Antivirus	2500	XX	XX	XX
	Other (Please Specify)	xx	XX	XX	XX
	<b>Total - A</b>		XX	XX	<b>XX</b>
	Note: Price to be quoted for Year One (1) only				

## Software ATS

	Software AMC/ATS	YEAR 2			YEAR 3			YEAR 4			YEAR 5			Total Amount for 5 yrs (INR)	GST	Grand Total
S. N.	Make /Model	Quantity (X)	Rate (INR) (Y)	Total Amount (INR) (X x Y)	Quantity (X)	Rate (INR) (Y)	Total Amount (INR) (X x Y)	Quantity (X)	Rate (INR) (Y)	Total Amount (INR) (X x Y)	Quantity (X)	Rate (INR) (Y)	Total Amount (INR) (X x Y)			
List of Software																
1	ACTIVE DIRECTORY MANAGEMENT SOLUTION	50000	XX	XX	50000	XX	XX	50000	XX	XX	50000	XX	XX	XX	XX	XX
2	PATCH AND ENDPOINT MANAGEMENT SOLUTION	45000	XX	XX	45000	XX	XX	45000	XX	XX	45000	XX	XX	XX	XX	XX
3	PATCHING OF RED HAT ENTERPRISE LINUX 8/9(RHEL 8/9) OPERATING SYSTEM ON IBM LINUXONE Z SYSTEMS WITH S390X ARCHITECTURE	800	XX	XX	800	XX	XX	800	XX	XX	800	XX	XX	XX	XX	XX
4	Red Hat VDC LICENSES Standard	10	XX	XX	10	XX	XX	10	XX	XX	10	XX	XX	XX	XX	XX
5	SFTP for DC and DRC with replication	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
6	Antivirus	2500	XX	XX	2500	XX	XX	2500	XX	XX	2500	XX	XX	XX	XX	XX
	Other (Please Specify)	XX			XX			XX			XX					
	Total - A			XX			XX			XX			XX	XX	XX	XXX

### Hardware Cost

Hardware Cost with Warranty							
S. N.	Make /Model	Details of the proposed hardware (The Details as required in the corresponding description column is to be provided for the proposed System software and hardware)	Quantity (X)	Rate (INR) (Y)	Total Amount (INR) (X x Y)	GST	Grand Total
Data Centre (DC)							
Server Hardware							
1	LOAD BALANCER	with 3 years warranty	2	XX	XX	XX	XX
2	Blanking Panel	1U Blanking Panel for 19inch Rack clip model tooless, made with high quality fire resistant material and power quoted finish, easily replacable and movable	300	XX	XX	XX	XX
	<b>Total - A</b>				XX	XX	XX
Disaster Recovery Centre (DRC)							
Server Hardware							
1	LOAD BALANCER	with 3 years warranty	2	XX	XX	XX	XX
2	Blanking Panel	1U Blanking Panel for 19inch Rack clip model tooless, made with high quality fire resistant material and power quoted finish, easily replacable and movable	300	XX	XX	XX	XX
	<b>Total - B</b>				XX	XX	XX
	<b>TOTAL A+B</b>				XX	XX	XX

### Hardware Installation Cost

HARDWARE INSTALLATION COST			YEAR 1				
S. N.	Make /Model	Details of the proposed hardware Installation Cost (The Details as required in the corresponding description column is to be provided for the proposed System software and hardware)	Quantity (X)	Rate (INR) (Y)	Total Amount (INR) (X x Y)	GST	Grand Total
Data Centre (DC)							
1	LOAD BALANCER		2	XX	XX	XX	XX
2	Blanking Panel		300	XX	XX	XX	XX
	<b>Total - A</b>				XX	XX	XX
Disaster Recovery Centre (DRC)							
1	LOAD BALANCER		2	XX	XX	XX	XX
2	Blanking Panel		300	XX	XX	XX	XX
	<b>Total - B</b>				XX	XX	XX
	<b>Grand Total =A+B</b>				XX	XX	XX



### Hardware AMC

	Hardware AMC Cost (Existing and New)		YEAR 1			YEAR 2 AMC			YEAR 3 AMC			YEAR 4 AMC			YEAR 5 AMC			Total AMC Cost (INR)	GST	Gran d Total
S. N.	Make /Model	Details of the Hardware with Start Date	Qt y	Rat e (IN R)	Total Amo unt (INR )	Qt y	Rat e (IN R)	Total Amo unt (INR )	Qt y	Rat e (IN R)	Total Amo unt (INR )	Qt y	Rate (INR)	Total Amo unt (INR )	Qt y	Rat e (IN R)	Total Amo unt (INR )			
Data Centre (DC)																				
Server Hardware																				
1	Oracle T8-1 Server	Serial No. - 2330NMC008 , 128GB RAM, Start Date - 13.08.2025	1	XX	XX	1	XX	XX	1	XX	XX	1	XX	XX	1	XX	XX	XX	XX	XX
2	LOAD Balancer											2	XX	XX	2	XX	XX	XX	XX	XX
	Total - A				XX			XX			XX			XX			xx	xx	xx	xx
Disaster Recovery Centre (DRC)																				
Server Hardware																				
1	Oracle T8-1 Server	Serial No. - 2330NMC007 , 128GB RAM, Start Date - 13.08.2025	1	XX	XX	1	XX	XX	1	XX	XX	1	XX	XX	1	XX	XX	XX	XX	XX
2	LOAD Balancer											2	XX	XX	2	XX	XX	XX	XX	XX
	Total - B				XX			XX			XX			XX			XX	XX	XX	XX
	TOTAL A+B				XX			XX			XX			XX			XX	XX	XX	XX

## FMS

FACILITY MANAGEMENT SERVICES																			
	FMS	Year -1			Year -2			Year -3			Year -4			Year -5			Total Cost for 5 years	GST	Grand Total
S. N.	Resources	No. of Resources (a)	Unit Rate (b)	Cost = (a x b)	No. of Resources (a)	Unit Rate (b)	Cost = (a x b)	No. of Resources (a)	Unit Rate (b)	Cost = (a x b)	No. of Resources (a)	Unit Rate (b)	Cost = (a x b)	No. of Resources (a)	Unit Rate (b)	Cost = (a x b)			
1	L2 (DC)	8	XX	XX	8	XX	XX	8	XX	XX	8	XX	XX	8	XX	XX	XX	XX	XX
2	L3 OEM NUTANIX	1	XX	XX	1	XX	XX	1	XX	XX	1	XX	XX	1	XX	XX	XX	XX	XX
3	L3 OEM AD MANAGEMENT	1	XX	XX	1	XX	XX	1	XX	XX	1	XX	XX	1	XX	XX	XX	XX	XX
4	L3 OEM PATCH MANAGEMENT	1	XX	XX	1	XX	XX	1	XX	XX	1	XX	XX	1	XX	XX	XX	XX	XX
																TOTAL	XX	XX	XX
1	Patch Management, AD Management System, SFTP, Antivirus			L2															
2	OEM / OEM Certified Engineer authorised by OEM for Patch Management System			L3															
3	OEM / OEM Certified Engineer authorised by OEM for AD Management System			L3															
4	OEM Engineer for NUTANIX System			L3															
	Note: FMS will start from the Date of Commissioning and acceptance of the Solution by Bank.																		

\*\*\*\*\***End of Document**\*\*\*\*\*