REQUEST FOR PROPOSAL (RFP)
FOR PROCUREMENT OF COMPREHENSIVE ENDPOINT SECURITY SOLUTION FOR STATE BANK GROUP

Ref: SBI/GITC/Platform Engineering-I/2021/2022/809

Dated: 06-Dec-2021

Deputy General Manager
IT-Platform Engineering-I Department,
State bank of India Global IT Centre,
Gr Floor 'A'- Wing, Plot no 8/9/10,
Sector -11, CBD Belapur
Navi Mumbai- 400614

Schedule of Events

Sl No	Particulars	Remarks
1	Contact details of issuing department (Name, Designation, Mobile No., Email and office address for sending any kind of correspondence regarding this RFP)	Name: Sunil Kumar Dadhich Designation: DGM (PE-I) Email ID: dgmit.pe1@sbi.co.in Contact Address: Deputy General Manager Platform Engineering- I Department, State Bank of India Global IT Centre, Ground Floor, 'A' Wing, CBD Belapur, Navi Mumbai-400614 Contact Number: 022-27565111 Mobile: 9413397539 Single point of contacts L1 Sh. Vijay Chourey, Manager (Systems), Mobile no. 8452926188 email: vijay.chourey@sbi.co.in, L2 Sh. Prashant Hari Wani, Mobile no. 9619665160 email: prashant.wani@sbi.co.in,
2	Bid Document Availability including changes/amendments, if any to be issued	RFP may be downloaded from Bank's website https://www.sbi.co.in procurement news and e-Procurement agency portal https://etender.sbi/SBI/ From 06.12.2021 to 06.01.2022
3	Last date for requesting clarification. Pre-Bid queries will be in format as per Appendix-L.	Up to 17.00 Hrs on 13.12.2021 All communications regarding points / queries requiring clarifications shall be given in writing or by e-mail.
4	Pre - bid Meeting at (venue)	From 16.00 Hrs to 17.00 Hrs on 20.12.2021 through online meeting
5	Clarifications to queries raised at pre-bid meeting will be provided by the Bank.	On 27.12.2021
6	Last date and time for Bid submission	Up to 16.00 Hrs. on **06.01.2022**
7	Address for submission of Bids	https://etender.sbi/SBI/
8	Date and Time of opening of Technical Bids	17.00 Hrs. on 06.01.2022 Authorized representatives of Bidders may be present online during opening of the Technical Bids. However,

		Technical Bids would be opened even in the absence of any or all of Bidders representatives.	
9	Opening of Indicative Price Bids	Indicative price bid of technically qualified bidders only will be opened on a subsequent date.	
10	Reverse Auction	On a subsequent date which will be communicated to such Bidders who qualify in the Technical Bid.	
11	Tender Fee (Refer para no 49 of this RFP)	Rs.25,000/- (Rupees Twenty-Five Thousand Only) Amount should be deposited in A/c No: 4897932113433 (NEFT Only) IFSC: SBIN0011343 Account Name: Subsidy Inward Remittance For RTGS or SBI to SBI Transfer A/c No: 37608352111 IFSC: SBIN0011343 Account Name: System Suspense Branch Parking A/C Tender fee will be non-refundable.	
12	Earnest Money Deposit (Refer para no 09 of this RFP)	NIL. In lieu of EMD, Bidders are required to submit Bid Security Declaration as per Technical Bid Form (Appendix-A). Bids without Bid Security Declaration under Technical Bid Form (Appendix-A) shall be summarily rejected.	
13	Bank Guarantee (Refer para no 24 of this RFP)	**03 %** of the Total project Cost.	Performance Security in form of BG should be valid for 05 (five) year(s) and 03 (three) months.
14	Contact details of e-Procurement agency appointed for e-procurement	E-Procurement Technologies Ltd. A-201/208, Wall Street – II, Opp. Orient Club, Ellisbridge, Ahmedabad – 380006 Gujarat e-Procurement agency portal https://etender.sbi/SBI/ Contact persons 1. Nandan Valera, Nandan.v@eptl.in,9081000427 2. Fahad Khan, Fahad@eptl.in, 9904406300	

Part-I

S.N.	INDEX
1	INVITATION TO BID
2	DISCLAIMER
3	DEFINITIONS
4	SCOPE OF WORK
5	ELIGIBILITY AND TECHNICAL CRITERIA
6	COST OF BID DOCUMENT
7	CLARIFICATIONS AND AMENDMENTS ON RFP/PRE-BID MEETING
8	CONTENTS OF BID DOCUMENTS
9	EARNEST MONEY DEPOSIT (EMD)
10	BID PREPARATION AND SUBMISSION
11	DEADLINE FOR SUBMISSION OF BIDS
12	MODIFICATION AND WITHDRAWAL OF BIDS
13	PERIOD OF BID VALIDITY AND VALIDITY OF PRICE QUOTED IN REVERSE AUCTION (RA)
14	BID INTEGRITY
15	BIDDING PROCESS/ OPENING OF TECHNICAL BIDS
16	TECHNICAL EVALUATION
17	EVALUATION OF INDICATIVE PRICE BIDS AND FINALIZATION
18	CONTACTING THE BANK
19	AWARD CRITERIA AND AWARD OF CONTRACT
20	POWER TO VARY OR OMIT WORK
21	WAIVER OF RIGHTS
22	CONTRACT AMENDMENT
23	BANK'S RIGHT TO ACCEPT ANY BID AND TO REJECT ANY OR ALL BIDS
24	BANK GUARANTEE
25	SYSTEM INTEGRATION TESTING & USER ACCEPTANCE TESTING
26	SERVICES
27	WARRANTY AND ANNUAL MAINTENANCE CONTRACT
28	PENALTIES
29	RIGHT TO VERIFICATION
30	INSPECTION AND TESTING
31	RIGHT TO AUDIT
32	SUB-CONTRACTING
33	VALIDITY OF AGREEMENT
34	LIMITATION OF LIABILITY
35	CONFIDENTIALITY
36	DELAY IN SERVICE PROVIDER'S PERFORMANCE
37	SERVICE PROVIDER'S OBLIGATIONS
38	TECHNICAL DOCUMENTATION
39	INTELLECTUAL PROPERTY RIGHTS AND OWNERSHIP
40	LIQUIDATED DAMAGES
41	CONFLICT OF INTEREST

42	CODE OF INTEGRITY AND DEBARMENT/BANNING
43	TERMINATION FOR DEFAULT
44	FORCE MAJEURE
45	TERMINATION FOR INSOLVENCY
46	TERMINATION FOR CONVENIENCE
47	DISPUTES AND ARBITRATION
48	GOVERNING LANGUAGES
49	APPLICABLE LAW
50	TAXES AND DUTIES
51	TAX DEDUCTION AT SOURCES
52	TENDER FEE
53	EXEMPTION OF EMD AND TENDER FEE
54	NOTICES

Part-II

Appendix	Index
A	BID FORM
B	BIDDER'S ELIGIBILITY CRITERIA
B1	SECURITY CONTROLS
C	TECHNICAL & FUNCTIONAL SPECIFICATIONS
D	BIDDER DETAILS
E	SCOPE OF WORK AND PAYMENT SCHEDULE
F	INDICATIVE PRICE BID
G	CERTIFICATE OF LOCAL CONTENT
H	BANK GUARANTEE FORMAT
I	PENALTIES
J	SERVICE LEVEL AGREEMENT
K	NON-DISCLOSURE AGREEMENT
L	PRE-BID QUERY FORMAT
M	FORMAT FOR SUBMISSION OF CLIENT REFERENCES
N	PRE-CONTRACT INTEGRITY PACT
O	OEM SECURED SOULTION CONFIRMATION

1. INVITATION TO BID:

i. **State Bank of India** (herein after referred to as **'SBI/the Bank')**, having its Corporate Centre at Mumbai, various other offices (LHOs/ Head Offices /Zonal Offices/Global Link Services, Global IT Centre, foreign offices etc.) of State Bank of India, branches/other offices, Subsidiaries and Joint Ventures available at various locations and managed by the Bank (collectively referred to as **State Bank Group or 'SBG'** hereinafter). This Request for Proposal (RFP) has been issued by **the Bank** on behalf of **SBG** for Procurement, Implementation, Integration, Maintenance, Administration, Onsite-Support and Licenses for Centralized Endpoint protection platform (EPP), Application Change Control (ACC), File Integrity Monitoring (FIM) and Early Detection and Response (EDR) as a comprehensive solution for **STATE BANK GROUP.** The overall project will be termed herein after as "**Endpoint Security Solution**" in this RFP.

ii. In order to meet the service requirements, the Bank proposes to invite online Bids from eligible Bidders as per details/scope of work mentioned in **Appendix-E** of this RFP.

iii. Bidder shall mean any entity (i.e. juristic person) who meets the eligibility criteria given in **Appendix-B** of this RFP and willing to provide the Services as required in this RFP. The interested Bidders who agree to all the terms and conditions contained in this RFP may submit their Bids with the information desired in this RFP. **Consortium bidding is not permitted** under this RFP.

iv. Address for submission of online Bids, contact details including email address for sending communications are given in Schedule of Events of this RFP.

v. The purpose of SBI behind this RFP is to seek a detailed technical and commercial proposal for procurement of the **S**ervice**s** desired in this RFP.

vi. This RFP document shall not be transferred, reproduced or otherwise used for purpose other than for which it is specifically issued.

vii. Interested Bidders are advised to go through the entire RFP before submission of online Bids to avoid any chance of elimination. The eligible Bidders desirous of taking up the project for providing of proposed **S**ervice**s** for SBI are invited to submit their technical and commercial proposal in response to this RFP. The criteria and the actual process of evaluation of the responses to this RFP and subsequent selection of the successful Bidder will be entirely at Bank's discretion. This RFP seeks proposal from Bidders who have the necessary experience, capability &

expertise to provide SBI the proposed **S**ervice**s** adhering to Bank's requirements outlined in this RFP.

2. **DISCLAIMER:**

i. The information contained in this RFP or information provided subsequently to Bidder(s) whether verbally or in documentary form/email by or on behalf of SBI, is subject to the terms and conditions set out in this RFP.

ii. This RFP is not an offer by State Bank of India, but an invitation to receive responses from the eligible Bidders.

iii. The purpose of this RFP is to provide the Bidder(s) with information to assist preparation of their Bid 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 contained in this RFP and where necessary obtain independent advices/clarifications. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

iv. The Bank, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form or arising in any way for participation in this bidding process.

v. The Bank also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP.

vi. The Bidder is expected to examine all instructions, forms, terms and specifications in this RFP. Failure to furnish all information required under this RFP or to submit a Bid not substantially responsive to this RFP in all respect will be at the Bidder's risk and may result in rejection of the Bid.

vii. The issue of this RFP does not imply that the Bank is bound to select a Bidder or to award the contract to the Selected Bidder, as the case may be, for the Project and the Bank reserves the right to reject all or any of the Bids or Bidders without assigning any reason whatsoever before issuance of purchase order and/or its acceptance thereof by the successful Bidder as defined in Award Criteria and Award of Contract in this RFP.

3. DEFINITIONS:

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

i. **"The Bank"** 'means the State Bank of India (including domestic branches and foreign offices), Subsidiaries and Joint Ventures, where the Bank has ownership of more than 50% of voting securities or the power to direct the management and policies of such Subsidiaries and Joint Ventures.

ii. **"Bidder/Channel Partner"** means an eligible entity/firm submitting the Bid in response to this RFP.

iii. **"Bid"** means the written reply or submission of response to this RFP.

iv. **"The Contract"** means the agreement entered into between the Bank and Service Provider, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

v. **"Total Contract Price/Project Cost/TCO"** means the price payable to Service Provider over the entire period of Contract for the full and proper performance of its contractual obligations.

vi. **"Vendor/Service Provider"** is the successful Bidder found eligible as per eligibility criteria set out in this RFP, whose technical Bid has been accepted and who has emerged as L1 (lowest in reverse auction) Bidder as per the selection criteria set out in the RFP and to whom notification of award has been given by the Bank.

vii. **"Services"** means all services, scope of work and deliverables to be provided by a Bidder as described in the RFP and include provision of technical assistance, training, certifications, auditing and other obligation of Service Provider covered under this RFP.

viii. **Software Solution/ Services/ System – "Software Solution" or "Services" or "System"** means all software products, services, scope of work and deliverables to be provided by a Bidder as described in the RFP and include services ancillary to the development of the solution, such as installation, commissioning, integration with existing systems, provision of technical assistance, training, certifications, auditing and other obligation of Service Provider covered under the RFP.

4. SCOPE OF WORK:

As given in **Appendix-E** of this document.

The Bank may, at its sole discretion, provide remote access to its information technology system to IT Service Provider through secured Virtual Private Network (VPN) in order to facilitate the performance of IT Services. Such remote access to the Bank's information technology system shall be subject to the following:

i. Service Provider shall ensure that the remote access to the Bank's VPN is performed through a laptop/desktop ("Device") specially allotted for that purpose by the Service Provider and not through any other private or public Device.

ii. Service Provider shall ensure that only its authorized employees/representatives access the Device.

iii. Service Provider shall be required to get the Device hardened/configured as per the Bank's prevailing standards and policy.

iv. Service Provider and/or its employee/representative shall be required to furnish an undertaking and/or information security declaration on the Bank's prescribed format before such remote access is provided by the Bank.

v. Service Provider shall ensure that services are performed in a physically protected and secure environment which ensures confidentiality and integrity of the Bank's data and artefacts, including but not limited to information (on customer, account, transactions, users, usage, staff, etc.), architecture (information, data, network, application, security, etc.), programming codes, access configurations, parameter settings, executable files, etc., which the Bank representative may inspect. Service Provider shall facilitate and/ or handover the Device to the Bank or its authorized representative for investigation and/or forensic audit.

vi. Service Provider shall be responsible for protecting its network and subnetworks, from which remote access to the Bank's network is performed, effectively against unauthorized access, malware, malicious code and other threats in order to ensure the Bank's information technology system is not compromised in the course of using remote access facility.

5. ELIGIBILITY AND TECHNICAL CRITERIA:

i. Bid is open to all Bidders who meet the eligibility and technical criteria as given in **Appendix-B, B1 & Appendix-C** of this document. The Bidder has to submit the documents substantiating eligibility criteria as mentioned in this RFP document.

(a) If any Bidder submits Bid on behalf of Principal/OEM, the same Bidder shall not submit a Bid on behalf of another Principal/OEM under the RFP. Bid submitted with option of multiple OEMs shall also be considered bid submitted on behalf of multiple OEM.

(b) Either the Bidder on behalf of Principal/OEM or Principal/OEM itself is allowed to Bid, however both cannot Bid simultaneously.

ii. The Bidder shall also submit **PRE-CONTRACT INTEGRITY PACT** along with technical Bid as prescribed in **Appendix-N** duly signed by the Bidder on each page and witnessed by two persons. The **Pre-Contract Integrity Pact** shall be stamped as applicable in the State where it is executed. **Bid submitted without Pre-Contract Integrity Pact, as per the format provided in the RFP, shall not be considered**.

6. COST OF BID DOCUMENT:

The participating Bidders shall bear all the costs associated with or relating to the preparation and submission of their Bids including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstration or presentations which may be required by the Bank or any other costs incurred in connection with or relating to their Bid. The Bank shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder regardless of the conduct or outcome of the bidding process.

7. CLARIFICATION AND AMENDMENTS ON RFP/PRE-BID MEETING:

i. Bidder requiring any clarification on RFP may notify the Bank in writing strictly as per the format given in **Appendix-L** at the address/by e-mail within the date/time mentioned in the Schedule of Events.

ii. A pre-Bid meeting will be held in person or online on the date and time specified in the Schedule of Events which may be attended by the authorized representatives of the Bidders interested to respond to this RFP.

iii. The queries received (without identifying source of query) and response of the Bank thereof will be posted on the Bank's website or conveyed to the Bidders.

iv. The Bank reserves the right to amend, rescind or reissue the RFP, at any time prior to the deadline for submission of Bids. The Bank, for any reason, whether, on its own initiative or in response to a clarification requested by a prospective Bidder, may modify the RFP, by amendment which will be made available to the Bidders by way of corrigendum/addendum. The interested parties/Bidders are advised to

check the Bank's website regularly till the date of submission of Bid document specified in the Schedule of Events/email and ensure that clarifications / amendments issued by the Bank, if any, have been taken into consideration before submitting the Bid. Such amendments/clarifications, if any, issued by the Bank will be binding on the participating Bidders. Bank will not take any responsibility for any such omissions by the Bidder. The Bank, at its own discretion, may extend the deadline for submission of Bids in order to allow prospective Bidders a reasonable time to prepare the Bid, for taking the amendment into account. Nothing in this RFP or any addenda/corrigenda or clarifications issued in connection thereto is intended to relieve Bidders from forming their own opinions and conclusions in respect of the matters addresses in this RFP or any addenda/corrigenda or clarifications issued in connection thereto.

v. No request for change in commercial/legal terms and conditions, other than what has been mentioned in this RFP or any addenda/corrigenda or clarifications issued in connection thereto, will be entertained and queries in this regard, therefore will not be entertained.

vi. Queries received after the scheduled date and time will not be responded/acted upon.

8. CONTENTS OF BID DOCUMENT:

i. The Bidder must thoroughly study/analyse and properly understand the contents of this RFP, its meaning and impact of the information contained therein.

ii. Failure to furnish all information required in this RFP or submission of Bid not responsive to this RFP in any respect will be at the Bidder's risk and responsibility and the same may finally result in rejection of its Bid. The Bank has made considerable effort to ensure that accurate information is contained in this RFP and is supplied solely as guidelines for Bidders.

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

iv. The information provided by the Bidders in response to this RFP will become the property of the Bank and will not be returned. Incomplete information in Bid document may lead to non-consideration of the proposal.

9. EARNEST MONEY DEPOSIT (EMD):

i. In lieu of EMD, Bidders are required to submit Bid Security Declaration as per Technical Bid Form (Appendix-A). Proposals without Bid Security Declaration

under Technical Bid Form (Appendix-A) shall be summarily rejected

ii. Bidder(s) shall be considered in breach of Bid Security Declaration :-

(a) if a Bidder withdraws his Bid during the period of Bid validity specified in this RFP; or

(b) if a technically qualified Bidder do not participate in the auction by not logging in, in the reverse auction tool; or

(c) if a Bidder makes any statement or encloses any form which turns out to be false / incorrect at any time prior to signing of Contract; or

(d) if the successful Bidder fails to accept Purchase Order and/or sign the Contract with the Bank or furnish Bank Guarantee, within the specified time period in the RFP.

iii. If Bid Security Declaration is breached for any reasons mentioned above, the concerned Bidder may be debarred from participating in the RFPs floated by the Bank/this department, in future, as per sole discretion of the Bank and other appropriate action may be initiated as per the terms of this RFP.

10. BID PREPARATION AND SUBMISSION:

i. The Bid is to be submitted separately for technical and Price on portal of e-Procurement agency for providing of **"**ENDPOINT SECURITY SOLUTION" for STATE BANK GROUP in response to the **RFP No. _____dated _____.** Documents mentioned below are to be uploaded on portal of e-Procurement agency with digital signature of authorised signatory:

(a) Index of all the documents, letters, bid forms etc. submitted in response to RFP along with page numbers.

(b) Bid covering letter/Bid form on the lines of **Appendix-A** on Bidder's letter head.

(c) Proof of remittance of Tender Fee as specified in this document.

(d) Specific response with supporting documents in respect of Eligibility Criteria as mentioned in **Appendix-B, B1** and technical eligibility criteria on the lines of **Appendix-C.**

(e) Bidder's details as per **Appendix-D** on Bidder's letter head.

(f) Audited financial statement and profit and loss account statement as mentioned in Part-II.

(g) A copy of board resolution along with copy of power of attorney (POA wherever applicable) showing that the signatory has been duly authorized to sign the Bid document.

(h) If applicable, scanned copy of duly stamped and signed Pre-Contract Integrity Pact subject to compliance of requirement mentioned in clause no 11(ii).

(i) If applicable, copy of registration certificate issued by competent authority as mentioned in Sl No 2 of Eligibility Criteria under Appendix-B.

ii. **Indicative Price Bid for** providing of **"**ENDPOINT SECURITY SOLUTION" for STATE BANK GROUP**" in** response to the **RFP No.** _____ dated _____should contain only indicative Price Bid strictly on the lines of **Appendix-F**. The Indicative Price must include all the price components mentioned. Prices are to be quoted in Indian Rupees only.

iii. Bidders may please note:

(a) The Bidder should quote for the entire package on a single responsibility basis for Services it proposes to supply.

(b) While submitting the Technical Bid, literature on the Services should be segregated and kept together in one section.

(c) Care should be taken that the Technical Bid shall not contain any price information. Such proposal, if received, will be rejected.

(d) The Bid document shall be complete in accordance with various clauses of the RFP document or any addenda/corrigenda or clarifications issued in connection thereto, duly signed by the authorized representative of the Bidder and stamped with the official stamp of the Bidder. Board resolution authorizing representative to Bid and make commitments on behalf of the Bidder is to be attached.

(e) It is mandatory for all the Bidders to have class-III Digital Signature Certificate (DSC) (in the name of person who will sign the Bid) from any of the licensed certifying agency to participate in this RFP. DSC should be in the name of the authorized signatory. It should be in corporate capacity (that is in Bidder capacity).

(f) Bids are liable to be rejected if only one Bid (i.e. Technical Bid or Indicative Price Bid) is received.

(g) If deemed necessary, the Bank may seek clarifications on any aspect from the Bidder. However, that would not entitle the Bidder to change or cause any change in the substances of the Bid already submitted or the price quoted.

(h) The Bidder may also be asked to give presentation for the purpose of clarification of the Bid.

(i) The Bidder must provide specific and factual replies to the points raised in the RFP.

(j) The Bid shall be typed or written and shall be digitally signed by the Bidder or a person or persons duly authorized to bind the Bidder to the Contract.

(k) All the enclosures (Bid submission) shall be serially numbered.

(l) Bidder(s) should prepare and submit their online Bids well in advance before the prescribed date and time to avoid any delay or problem during the bid submission process. The Bank shall not be held responsible for any sort of delay or the difficulties faced by the Bidder(s) during the submission of online Bids.

(m) Bidder(s) should ensure that the Bid documents submitted should be free from virus and if the documents could not be opened, due to virus or otherwise, during Bid opening, the Bid is liable to be rejected.

(n) The Bank reserves the right to reject Bids not conforming to above.

11. DEADLINE FOR SUBMISSION OF BIDS:

i. Bids must be submitted online on portal of e-Procurement agency by the date and time mentioned in the "Schedule of Events".

ii. Wherever applicable, the Bidder shall submit the original EMD Bank Guarantee and Pre- Contract Integrity Pact together with their respective enclosures and seal it in an envelope and mark the envelope as "Technical Bid". The said envelope shall clearly bear the name of the project and name and address of the Bidder. In addition, the last date for bid submission should be indicated on the right and corner of the envelope. The original documents should be submitted within the bid submission date and time for the RFP at the address mentioned in Sl No 1 of Schedule of Events, failing which Bid will be treated as non-responsive.

iii. In the event of the specified date for submission of Bids being declared a holiday for the Bank, the Bids will be received up to the appointed time on the next working day.

iv. In case the Bank extends the scheduled date of submission of Bid document, the Bids shall be submitted by the time and date rescheduled. All rights and obligations of the Bank and Bidders will remain the same.

12. MODIFICATION AND WITHDRAWAL OF BIDS:

i. The Bidder may modify or withdraw its Bid after the Bid's submission, provided modification, including substitution or withdrawal of the Bids, is received on e-procurement portal, prior to the deadline prescribed for submission of Bids.

ii. No modification in the Bid shall be allowed, after the deadline for submission of Bids.

iii. No Bid shall be withdrawn in the interval between the deadline for submission of Bids and the expiration of the period of Bid validity specified in this RFP.

Withdrawal of a Bid during this interval may result in appropriate action as per the terms of this RFP.

13. PERIOD OF BID VALIDITY AND VALIDITY OF PRICE QUOTED IN REVERSE AUCTION (RA):

i. Bid shall remain valid for duration of 6 calendar months from Bid submission date.

ii. Price quoted by the Bidder in Reverse auction shall remain valid for duration of 6 calendar months from the date of conclusion of RA.

iii. In exceptional circumstances, the Bank may solicit the Bidders' consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. A Bidder is free to refuse the request. However, in such case, the Bid Security Declaration shall not be treated as breached. However, any extension of validity of Bids or price will not entitle the Bidder to revise/modify the Bid document.

iv. Once Purchase Order or Letter of Intent is issued by the Bank, the said price will remain fixed for the entire Contract period and shall not be subjected to variation on any account, including exchange rate fluctuations and custom duty. A Bid submitted with an adjustable price quotation will be treated as non-responsive and will be rejected.

14. BID INTEGRITY:

Willful misrepresentation of any fact within the Bid will lead to the cancellation of the contract without prejudice to other actions that the Bank may take. All the submissions, including any accompanying documents, will become property of the Bank. The Bidders shall be deemed to license, and grant all rights to the Bank, to reproduce the whole or any portion of their Bid document for the purpose of evaluation and to disclose the contents of submission for regulatory and legal requirements.

15. BIDDING PROCESS/OPENING OF TECHNICAL BIDS:

i. All the technical Bids received up to the specified time and date will be opened for initial evaluation on the time and date mentioned in the schedule of events. The technical Bids will be opened in the presence of representatives of the Bidders who choose to attend the same on portal of e-Procurement agency. However, Bids may be opened even in the absence of representatives of one or more of the Bidders.

ii. In the first stage, only technical Bid will be opened and evaluated. Bids of such

Bidders satisfying eligibility criteria and agree to comply with all the terms and conditions specified in the RFP will be evaluated for technical criteria/specifications/eligibility. Only those Bids complied with technical criteria shall become eligible for indicative price Bid opening and further RFP evaluation process.

iii. The Bank will examine the Bids to determine whether they are complete, required formats have been furnished, the documents have been properly signed, Tender Fee for the desired amount and validity period is available and the Bids are generally in order. The Bank may, at its discretion waive any minor non-conformity or irregularity in a Bid which does not constitute a material deviation.

iv. Prior to the detailed evaluation, the Bank will determine the responsiveness of each Bid to the RFP. For purposes of these Clauses, a responsive Bid is one, which conforms to all the terms and conditions of the RFP in toto, without any deviation.

v. The Bank's determination of a Bid's responsiveness will be based on the contents of the Bid itself, without recourse to extrinsic evidence.

vi. After opening of the technical Bids and preliminary evaluation, some or all the Bidders may be asked to make presentations on the Service proposed to be offered by them.

vii. If a Bid is not responsive, it will be rejected by the Bank and will not subsequently be made responsive by the Bidder by correction of the non-conformity.

16. TECHNICAL EVALUATION:

i. Technical evaluation will include technical information submitted as per technical Bid format, demonstration of proposed Services, reference calls and site visits, wherever required. The Bidder may highlight the noteworthy/superior features of their Services. The Bidder will demonstrate/substantiate all claims made in the technical Bid along with supporting documents to the Bank, the capability of the Services to support all the required functionalities at their cost in their lab or those at other organizations where similar Services is in use.

ii. During evaluation and comparison of Bids, the Bank may, at its discretion ask the Bidders for clarification on the Bids received. The request for clarification shall be in writing and no change in prices or substance of the Bid shall be sought, offered or permitted. No clarification at the initiative of the Bidder shall be entertained after bid submission date.

17. EVALUATION OF INDICATIVE PRICE BIDS AND FINALIZATION:

i. The indicative price Bid(s) of only those Bidders, who are short-listed after technical evaluation, would be opened.

ii. All the Bidders who qualify in the evaluation process shall have to participate in the online reverse auction to be conducted by Bank's authorized service provider on behalf of the Bank.

iii. Shortlisted Bidders shall be willing to participate in the reverse auction process and must have a valid digital signature certificate. Such Bidders will be trained by Bank's authorized e-Procurement agency for this purpose. Bidders shall also be willing to abide by the e-business rules for reverse auction framed by the Bank / Authorised e-Procurement agency. The details of e-business rules, processes and procedures will be provided to the short-listed Bidders.

iv. The Bidder will be selected as L1 on the basis of net total of the price evaluation as quoted in the Reverse Auction.

v. The successful Bidder is required to provide price confirmation and price breakup strictly on the lines of **Appendix-F** within 48 hours of conclusion of the Reverse Auction, failing which Bank may take appropriate action.

vi. Errors, if any, in the price breakup format will be rectified as under:

(a) If there is a discrepancy between the unit price and total price which is obtained by multiplying the unit price with quantity, the unit price shall prevail, and the total price shall be corrected unless it is a lower figure. If the Bidder does not accept the correction of errors, the Bid will be rejected.

(b) If there is a discrepancy in the unit price quoted in figures and words, the unit price in figures or in words, as the case may be, which corresponds to the total Bid price for the Bid shall be taken as correct.

(c) If the Bidder has not worked out the total Bid price or the total Bid price does not correspond to the unit price quoted either in words or figures, the unit price quoted in words shall be taken as correct.

(d) The Bidder should quote for all the items/services desired in this RFP. In case, prices are not quoted by any Bidder for any specific product and / or service, for the purpose of evaluation, the highest of the prices quoted by other Bidders participating in the bidding process will be reckoned as the notional price for that service, for that Bidder. However, if selected, at the time of award of Contract, the lowest of the price(s) quoted by other Bidders (whose Price Bids are also

opened) for that service will be reckoned. This shall be binding on all the Bidders. However, the Bank reserves the right to reject all such incomplete Bids.

18. CONTACTING THE BANK:

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

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

19. AWARD CRITERIA AND AWARD OF CONTRACT:

i. **Applicability of Preference to Make in India, Order 2017 (PPP-MII Order)**

Guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order) and any revision thereto will be applicable for this RFP and allotment will be done in terms of said Order as under:

(a) Among all qualified bids, the lowest bid (as quoted in reverse auction) will be termed as L1. If L1 is 'Class-I local supplier', the contract will be awarded to L1.

(b) If L1 is not from a '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.

(c) 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, then the contract will be awarded to the L1 bidder.

For the purpose of Preference to Make in India, Order 2017 (PPP-MII Order) and revision thereto:

"Local content" means the amount of value added in India which shall, unless otherwise prescribed by the Nodal Ministry, be the total value of the item procured

(excluding net domestic indirect taxes) minus the value of imported content in the item (including all customs duties) as a proportion of the total value, in percent.

"Class-I local supplier" means a supplier or service provider whose product or service offered for procurement meets the minimum local content as prescribed for 'Class-I local supplier' hereunder.

"Class-II local supplier" means a supplier or service provider whose product or service offered for procurement meets the minimum local content as prescribed for 'Class-II local supplier' hereunder. Class-II local supplier shall not get any purchase preference under this RFP.

"Non-local supplier" means a supplier or service provider whose product or service offered for procurement has 'local content' less than that prescribed for 'Class-II local supplier' under this RFP.

"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.

"Margin of purchase preference" means the maximum extent to which the price quoted by a 'Class-I local supplier' may be above the L1 for the purpose of purchase preference. The margin of purchase preference shall be 20%.

ii. **Verification of local content**

The 'Class-I local supplier'/ 'Class-II local supplier' at the time of submission of bid shall be required to provide a certificate as per **Appendix-G** 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 requirement for 'Class-I local supplier'/ 'Class-II local supplier' as the case may be.

iii. Total cost of Services along with cost of all items specified in **Appendix-F** would be the Total Cost of Ownership (TCO)/Total Project Cost and should be quoted by the Bidder(s) in indicative price bid and reverse auction.

iv. Bank will notify successful Bidder in writing by way of issuance of purchase order through letter or fax/email that its Bid has been accepted. The selected Bidder has

to return the duplicate copy of the same to the Bank within ***7* working days**, duly Accepted, Stamped and Signed by Authorized Signatory in token of acceptance.

v. The successful Bidder will have to submit Non-disclosure Agreement, Bank Guarantee for the amount and validity as desired in this RFP and strictly on the lines of format given in Appendix of this RFP together with acceptance of all terms and conditions of RFP.

vi. Copy of board resolution and power of attorney (POA wherever applicable) showing that the signatory has been duly authorized to sign the acceptance letter, contract and **NDA** should be submitted.

vii. The successful Bidder shall be required to enter into a Contract with the Bank and submit the Bank Guarantee, within 30 days from issuance of Purchase Order or within such extended period as may be decided by the Bank.

viii. Till execution of a formal contract, the RFP, along with the Bank's notification of award by way of issuance of purchase order and Service Provider's acceptance thereof, would be binding contractual obligation between the Bank and the successful Bidder.

ix. The Bank reserves the right to stipulate, at the time of finalization of the Contract, any other document(s) to be enclosed as a part of the final Contract.

x. Failure of the successful Bidder to comply with the requirements/terms and conditions of this RFP shall constitute sufficient grounds for the annulment of the award and forfeiture of the BG.

xi. Upon notification of award to the successful Bidder, the Bank will promptly notify the award of contract to the successful Bidder on the Bank's website.

20. POWERS TO VARY OR OMIT WORK:

i. No alterations, amendments, omissions, additions, suspensions or variations of the work (hereinafter referred to as variation) under the contract shall be made by the successful Bidder except as directed in writing by Bank. The Bank shall have full powers, subject to the provision herein after contained, from time to time during the execution of the contract, by notice in writing to instruct the successful Bidder to make any variation without prejudice to the contract. The finally selected Bidder shall carry out such variation and be bound by the same conditions as far as applicable as though the said variations occurred in the contract documents. If any, suggested variations would, in the opinion of the finally selected Bidder, if carried out, prevent him from fulfilling any of his obligations under the contract, he shall

notify Bank thereof in writing with reasons for holding such opinion and Bank shall instruct the successful Bidder to make such other modified variation without prejudice to the contract. The finally selected Bidder shall carry out such variation and be bound by the same conditions as far as applicable as though the said variations occurred in the contract documents. If the Bank confirms its instructions, the successful Bidder's obligations shall be modified to such an extent as may be mutually agreed, if such variation involves extra cost. Any agreed difference in cost occasioned by such variation shall be added to or deducted from the contract price as the case may be.

ii. In any case in which the successful Bidder has received instructions from the Bank as to the requirements for carrying out the altered or additional substituted work which either then or later on, will in the opinion of the finally selected Bidders, involve a claim for additional payments, such additional payments shall be mutually agreed in line with the terms and conditions of the order.

iii. If any change in the work is likely to result in reduction in cost, the parties shall agree in writing so as to the extent of change in contract price, before the finally selected Bidder(s) proceeds with the change.

21. WAIVER OF RIGHTS:

Each Party agrees that any delay or omission on the part of the other Party to exercise any right, power or remedy under this RFP will not automatically operate as a waiver of such right, power or remedy or any other right, power or remedy and no waiver will be effective unless it is in writing and signed by the waiving Party. Further the waiver or the single or partial exercise of any right, power or remedy by either Party hereunder on one occasion will not be construed as a bar to a waiver of any successive or other right, power or remedy on any other occasion.

22. CONTRACT AMENDMENT:

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

23. BANK'S RIGHT TO ACCEPT ANY BID AND TO REJECT ANY OR ALL BIDS:

The Bank reserves the right to accept or reject any Bid in part or in full or to cancel the bidding process and reject all Bids at any time prior to contract award as specified in Award Criteria and Award of Contract, without incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for the Bank's action.

24. BANK GUARANTEE:

i. Performance security in form of Bank Guarantee [BG] for the amount with validity period as specified in this RFP strictly on the format at **Appendix-H** is to be submitted by the finally selected Bidder (s). The BG has to be issued by a Scheduled Commercial Bank other than SBI and needs to be submitted within the specified time of receipt of formal communication from the Bank about their Bid finally selected. In case, SBI is the sole Banker for the Bidder, a Letter of Comfort from SBI may be accepted.

ii. The Bank Guarantee is required to protect interest of the Bank against the risk of non-performance of Service Provider in respect of successful implementation of the project and/or failing to perform / fulfil its commitments / obligations in respect of providing Services as mentioned in this RFP; or breach of any terms and conditions of the RFP, which may warrant invoking of Bank Guarantee.

25. SYSTEM INTEGRATION TESTING & USER ACCEPTANCE TESTING:

Service Provider should integrate the software with the existing systems as per requirement of the Bank and carry out thorough system integration testing.

System integration testing will be followed by user acceptance testing, plan for which has to be submitted by Service Provider to the Bank. The UAT includes functional tests, resilience tests, benchmark comparisons, operational tests, load tests etc. SBI staff / third Party vendor designated by the Bank will carry out the functional testing. This staff / third party vendor will need necessary on-site training for the purpose and should be provided by Service Provider. Service Provider should carry out other testing like resiliency/benchmarking/load etc. Service Provider should submit result log for all testing to the Bank.

On satisfactory completion of the aforementioned tests, the User Acceptance Test (UAT) letter will be issued to Service Provider by the competent authority on the line of **Appendix-I**.

26. SERVICES:

a. Service Provider should ensure that the quality of methodologies for delivering the services, adhere to quality standards/timelines stipulated therefor.

b. Service Provider support staff should be well trained to effectively handle queries raised by the customers/employees of the Bank.

c. Updated escalation matrix shall be made available to the Bank once in each quarter and each time the matrix gets changed.

d. Service provider should be responsible for support, services, software licenses, hardware management, maintenance, AMC during the contract period.

e. All professional services necessary to successfully implement the proposed solution will be part of the RFP/Contract.

f. The Bidder should also submit as part of technical Bid an overview of Project Management approach of the proposed product.

g. Bidder should ensure that key personnel with relevant skill sets are available to the Bank.

h. Bidder should ensure that the quality of methodologies for delivering the services, adhere to quality standards/timelines stipulated therefor.

i. Bidder shall be willing to transfer skills to relevant personnel from the Bank, by means of training and documentation.

j. Bidder shall provide and implement patches/ upgrades/ updates for hardware/ software/ Operating System / Middleware etc. as and when released by Service Provider/ OEM or as per requirements of the Bank. Bidder should bring to notice of the Bank all releases/ version changes.

k. Bidder shall obtain a written permission from the Bank before applying any of the patches/ upgrades/ updates. Bidder has to support older versions of the hardware/ software/ Operating System /Middleware etc. in case the Bank chooses not to upgrade to latest version.

l. Bidder shall provide AMC/maintenance support for Hardware/ Software/ Operating System/ Middleware over the entire period of contract.

m. All product updates, upgrades & patches shall be provided by the Bidder/ Service Provider free of cost during warranty period of 05 years (i.e. contract period of project) and AMC/ ATS/ S&S period.

n. Bidder shall provide legally valid Software Solution. The detailed information on license count and type of license shall also be provided to the Bank.

o. The Bidder shall keep the Bank explicitly informed the end of support dates on related products/hardware/firmware and should ensure support during warranty period of 05 years (i.e. contract period of project) and AMC/ATS/S&S.

p. The bidder shall provide or arrange the experts in operating systems (windows and non-windows), database oracle, MS sql any other DB and any other software/tool used in their solution or in support of solution for troubleshooting /installation/management/maintenance during the contract period.

27. WARRANTY AND ANNUAL MAINTENANCE CONTRACT:

i. The selected Bidder shall support the Software Solution during the period of warranty and AMC (if included in purchase order) as specified in Scope of work in this RFP from the date of acceptance of the Software Solution by State Bank of India.

ii. During the warranty and AMC period (if desired), the Bidder will have to undertake comprehensive support of the Software Solution supplied by the Bidder and all new versions, releases, and updates for all standard software to be supplied to the Bank at no additional cost . During the support period, the Bidder shall maintain the Software Solution to comply with parameters defined for acceptance criteria and the Bidder shall be responsible for all costs relating to labour, spares, maintenance (preventive and corrective), compliance of security requirements and transport charges from and to the Site (s) in connection with the repair/ replacement of the Software Solution, which, under normal and proper use and maintenance thereof, proves defective in design, material or workmanship or fails to conform to the specifications, as specified.

iii. During the support period (warranty and AMC, if desired), Service Provider shall ensure that services of professionally qualified personnel are available for providing comprehensive on-site maintenance of the Software Solution and its components as per the Bank's requirements. Comprehensive maintenance shall include, among other things, day to day maintenance of the Software Solution as per the Bank's policy, reloading of firmware/software, compliance to security requirements, etc. when required or in the event of system crash/malfunctioning, arranging and configuring facility as per the requirements of the Bank, fine tuning, system monitoring, log maintenance, etc. The Bidder shall provide services of an expert engineer at SBI GITC, Belapur or at other locations wherever required, whenever it is essential. In case of failure of Software Solution, the Bidder shall ensure that

Software Solution is made operational to the full satisfaction of the Bank within the given timelines.

iv. Warranty/ AMC (if opted) for the system software/ off-the shelf software will be provided to the Bank as per the general conditions of sale of such software.

v. Support (Warranty/ AMC, if opted) would be on-site and comprehensive in nature and must have back to back support from the OEM/Service Provider. Service Provider will warrant products against defects arising out of faulty design etc. during the specified support period.

vi. In the event of system break down or failures at any stage, protection available, which would include the following, shall be specified.
    (a) Diagnostics for identification of systems failures
    (b) Protection of data/ Configuration
    (c) Recovery/ restart facility
    (d) Backup of system software/ Configuration

vii. Prompt support shall be made available as desired in this RFP during the support period at the locations as and when required by the Bank.

viii. The Bidder shall be agreeable for on-call/on-site support during peak weeks (last and first week of each month) and at the time of switching over from PR to DR and vice-versa. No extra charge shall be paid by the Bank for such needs, if any, during the support period.

ix. Bidder support staff should be well trained to effectively handle queries raised by the customers/employees of the Bank.

x. Updated escalation matrix shall be made available to the Bank once in each quarter and each time the matrix gets changed.

28. PENALTIES:

As mentioned in **Appendix-I** of this RFP.

29. RIGHT TO VERIFICATION:

The Bank reserves the right to verify any or all of the statements made by the Bidder in the Bid document and to inspect the Bidder's facility, if necessary, to establish to its satisfaction about the Bidder's capacity/capabilities to perform the job.

30. INSPECTION AND TESTING:

i. The Bank reserves the right to carry out pre-shipment inspection or demand a demonstration of the product on a representative model at Service Provider's location.

ii. The inspection and test prior to dispatch of the product/at the time of final acceptance would be as follows:

(a) Service Provider shall intimate the Bank before dispatching products for conducting inspection and testing.

(b) The inspection and acceptance test may also be conducted at the point of delivery and / or at the products' final destination. Reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors, at no charge to the Bank. In case of failure by Service Provider to provide necessary facility / equipment at its premises, all the cost of such inspection like travel, boarding, lodging & other incidental expenses of the Bank's representatives to be borne by Service Provider.

iii. The Bank's right to inspect, test the product/ solution after delivery of the same to the Bank and where necessary reject the products/solution which does not meet the specification provided by the Bank. This shall in no way be limited or waived by reason of the products/ solution having previously being inspected, tested and passed by the Bank or its representative prior to the products/ solution shipment from the place of origin by the Bank or its representative prior to the installation and commissioning.

iv. Nothing stated hereinabove shall in any way release Service Provider from any warranty or other obligations under this contract.

v. System integration testing and User Acceptance testing will be carried out as per requirement of the Bank.

31. RIGHT TO AUDIT:

i. The Selected Bidder (Service Provider) shall be subject to annual audit by internal/ external Auditors appointed by the Bank/ inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ Software) and services etc. provided to the Bank and Service Provider is required to submit such certification by such Auditors to the Bank. Service Provider and or his / their outsourced agents / sub – contractors (if allowed by the Bank) shall facilitate the same The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created

by Service Provider. Service Provider shall, whenever required by the Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the Bank. Except for the audit done by Reserve Bank of India or any statutory/regulatory authority, the Bank shall provide reasonable notice not less than 7 (seven) days to Service Provider before such audit and same shall be conducted during normal business hours.

ii. Where any deficiency has been observed during audit of Service Provider on the risk parameters finalized by the Bank or in the certification submitted by the Auditors, Service Provider shall correct/resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies. The resolution provided by Service Provider shall require to be certified by the Auditors covering the respective risk parameters against which such deficiencies have been observed.

iii. Service Provider further agrees that whenever required by the Bank, it will furnish all relevant information, records/data to such auditors and/or inspecting officials of the Bank/Reserve Bank of India and/or any regulatory authorities. The Bank reserves the right to call for and/or retain any relevant information /audit reports on financial and security review with their findings undertaken by Service Provider. However, Service Provider shall not be obligated to provide records/data not related to Services under the Agreement (e.g. internal cost breakup etc.).

32. SUBCONTRACTING:

As per scope of this RFP, **sub-contracting is not permitted**.

33. VALIDITY OF AGREEMENT:

The Agreement/ SLA will be valid for the period of **Five** years from the date of complete implementation/rollout of solution at Bank level. The Bank reserves the right to terminate the Agreement as per the terms of RFP/ Agreement.

34. LIMITATION OF LIABILITY:

i. The maximum aggregate liability of Service Provider, subject to clause *31 (iii)*, in respect of any claims, losses, costs or damages arising out of or in connection with this RFP/Agreement shall not exceed the total Project Cost.

ii. Under no circumstances shall either Party be liable for any indirect, consequential or incidental losses, damages or claims including loss of profit, loss of business or revenue.

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

(a) claims that are the subject of indemnification pursuant to infringement of third-party Intellectual Property Right;
(b) damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider,
(c) damage(s) occasioned by Service Provider for breach of Confidentiality Obligations,
(d) Regulatory or statutory fines imposed by a Government or Regulatory agency for non-compliance of statutory or regulatory guidelines applicable to the Bank, provided such guidelines were brought to the notice of Service Provider.

For the purpose of clause *31(iii)(b)* **"Gross Negligence" means** any act or failure to act by a party which was in reckless disregard of or gross indifference to the obligation of the party under this Agreement and which causes injury, damage to life, personal safety, real property, harmful consequences to the other party, which such party knew, or would have known if it was acting as a reasonable person, would result from such act or failure to act for which such Party is legally liable. Notwithstanding the forgoing, Gross Negligence shall not include any action taken in good faith.
"Willful Misconduct" means any act or failure to act with an intentional disregard of any provision of this Agreement, which a party knew or should have known if it was acting as a reasonable person, which would result in injury, damage to life, personal safety, real property, harmful consequences to the other party, but shall not include any error of judgment or mistake made in good faith.

35. CONFIDENTIALITY:

Confidentiality obligation shall be as per Non-disclosure agreement and clause 14 of Service Level Agreement placed as Appendix to this RFP.

The Bank reserves its right to recall all the Bank's materials including Confidential Information, if stored in Service Provider system or environment, at any time during the term of the Contract or immediately upon expiry or termination of Contract. Service Provider shall ensure complete removal of such material or data from its system or environment (including backup media) to the satisfaction of the Bank.

36. DELAY IN SERVICE PROVIDER'S PERFORMANCE:

i. Services shall be made by Service Provider within the timelines prescribed in part II of this document.

ii. If at any time during performance of the Contract, Service Provider should

encounter conditions impeding timely delivery and performance of Services, Service Provider shall promptly notify the Bank in writing of the fact of the delay, its likely duration and cause(s). As soon as practicable after receipt of Service Provider's notice, the Bank shall evaluate the situation and may, at its discretion, extend Service Providers' time for performance, in which case, the extension shall be ratified by the parties by amendment of the Contract.

iii. Any delay in performing the obligation/ defect in performance by Service Provider may result in imposition of penalty, liquidated damages, invocation of Bank Guarantee and/or termination of Contract (as laid down elsewhere in this RFP document).

37. SERVICE PROVIDER'S OBLIGATIONS:

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

ii. Service Provider is obliged to work closely with the Bank's staff, act within its own authority and abide by directives issued by the Bank from time to time and complete implementation activities.

iii. Service Provider will abide by the job safety measures prevalent in India and will free the Bank from all demands or responsibilities arising from accidents or loss of life, the cause of which is Service Provider's negligence. Service Provider will pay all indemnities arising from such incidents and will not hold the Bank responsible or obligated.

iv. Service Provider is responsible for activities of its personnel or sub-contracted personnel (where permitted) and will hold itself responsible for any misdemeanours.

v. Service Provider shall treat as confidential all data and information about the Bank, obtained in the process of executing its responsibilities, in strict confidence and will not reveal such information to any other party without prior written approval of the Bank as explained under '**Non-Disclosure Agreement'** in **Appendix-K** of this RFP.

vi. Without the Bank's prior written permission, Service Provider shall not store or share Bank's materials including Confidential Information outside the geographical boundary of India or in/with a public cloud.

vii. Service Provider agrees that the Bank either itself or through its authorized representative shall have right to perform ethical hacking on public IPs and URLs of Service Provider, wherein the Bank has integrations.

viii. Service Provider agrees that it shall communicate to the Bank well in advance along with detail plan of action, if any changes in Service Provider's environment/infrastructure is of the nature that may have direct or indirect impact on the Services provided under this Agreement or operations of its Services.

ix. Service Provider at its own expenses, agrees to provide audit report of the process and infrastructure from CERT-In empanelled ISSP, periodically, at least once in a year or as requested by the Bank.

x. Service Provider shall ensure confidentiality, integrity and availability of the Bank's information at all times and shall comply with regard to the followings:
   (a) Acceptable Usage Policy: Information assets of Service Provider should be provided to its authorized users only for the intended purpose and users shall adhere to safe and acceptable usage practices.
   (b) Email Usage: The employees of Service Provider shall use authorized media only for email communication.
   (c) Password Management: Service Provider shall have a password management system in place, which ensures secure passwords.
   (d) Physical and Environmental Security: Service Provider shall provide sufficient guidance for its employees with respect to physical and environmental security.
   (e) Logical Access Control and User Access Management: The access to information and information systems shall be according to the principles of "least privilege" and "need to know" basis to authorized users of Service Provider.
   (f) Infrastructure Security: Service Provider shall ensure correct and secure operations of information processing facilities.
   (g) Change Management: Service Provider shall provide a managed and orderly method in which changes to the information technology environment are requested, tested and approved prior to installation or implementation.
   (h) Information Security Incident Management: Service provider shall ensure effective management of information security incidents, including the preservation of digital evidence.
   (i) Communications Strategy: Service provider shall ensure prevention of unauthorized access to communications traffic, or to any written information that is transmitted or transferred.
   (j) Service Provider Relationship: Service provider shall ensure that information security risks related to outsourcing of Services to any other party, if permitted by the Bank, shall be assessed and managed regularly, to the satisfaction of the Bank.

(k) Digital Risk: Service Provider shall ensure that electronic data is gathered and preserved in a systematic, standardized and legal manner to ensure the admissibility of the evidence for the purpose of any legal proceedings or investigations, whenever demanded by the Bank.

(l) Change Management: Service Provider shall provide a managed and orderly method in which changes to the information technology environment (including, database, operating system, application, networking etc.) are requested, tested and approved prior to installation or implementation.

(m) Port Management: Service Provider shall ensure that the controls are implemented for secure port management so as to protect the network from unauthorized access.

(n) Patch Management: Service Provider shall ensure that the security patches to information assets and systems are correctly and completely updated in a timely manner for known vulnerabilities.

(o) Backup Management: Service Provider shall ensure that regular backup is taken so that when necessary, information may be restored from backup media to return the application, database, operating system etc. to production status.

(p) Access Management: Service Provider shall limit access to information and information processing facilities for authorized users only.

(q) Log Management: Logging shall be enabled on all systems of Service Provider to ensure audit trail is maintained every time.

(r) Service Provider shall have an anti-virus solution with regular updates to protect their system against malicious attacks in the form of virus, malware, trojans etc.

38. TECHNICAL DOCUMENTATION:

i. Service Provider shall provide documents related to review records/ Test Bug Reports/ Root Cause Analysis Report, list of all Product components, list of all dependent/external modules and list of all documents relating to traceability of service level failure as and when applicable.

ii. Service Provider shall also provide the MIS reports as per requirements of the Bank. Any level/ version changes and/or clarification or corrections or modifications in the above-mentioned documentation should be supplied by Service Provider to the Bank, free of cost in timely manner.

iii. Service provider shall also provide the documents/SOP/Manual and also prepare the documents/SOP/Manual/reports in Bank prescribed formats as and when required by the Bank during the contract period.

39. INTELLECTUAL PROPERTY RIGHTS AND OWNERSHIP:

i. For any technology / software / product used by Service Provider for performing

Services for the Bank as part of this RFP, Service Provider shall have right to use as well as right to license such technology/ software / product. The Bank shall not be liable for any license or IPR violation on the part of Service Provider.

ii. Without the Bank's prior written approval, Service provider will not, in performing the Services, use or incorporate link to or call or depend in any way upon, any software or other intellectual property that is subject to an Open Source or Copy left license or any other agreement that may give rise to any third-party claims or to limit the Bank's rights under this RFP.

iii. Subject to clause *36 (iv) and 36 (v)* of this RFP, Service Provider shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the Bank against all costs, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from the Services or use of the technology / software / products or any part thereof in India or abroad.

iv. The Bank will give (a) notice to Service Provider of any such claim without delay/provide reasonable assistance to Service Provider in disposing of the claim; (b) sole authority to defend and settle such claim and; (c) will at no time admit to any liability for or express any intent to settle the claim provided that (i) Service Provider shall not partially settle any such claim without the written consent of the Bank, unless such settlement releases the Bank fully from such claim, (ii) Service Provider shall promptly provide the Bank with copies of all pleadings or similar documents relating to any such claim, (iii) Service Provider shall consult with the Bank with respect to the defence and settlement of any such claim, and (iv) in any litigation to which the Bank is also a party, the Bank shall be entitled to be separately represented at its own expenses by counsel of its own selection.

v. Service Provider shall have no obligations with respect to any infringement claims to the extent that the infringement claim arises or results from: (i) Service Provider's compliance with the Bank's specific technical designs or instructions (except where Service Provider knew or should have known that such compliance was likely to result in an infringement claim and Service Provider did not inform the Bank of the same); or (ii) any unauthorized modification or alteration of the deliverable (if any) by the Bank.

vi. All information processed by Service provider during Services belongs to the Bank. Service provider shall not acquire any other right in respect of the information for the license to the rights owned by the Bank. Service provider will implement mutually agreed controls to protect the information. Service provider also agrees that it will protect the information appropriately.

40. LIQUIDATED DAMAGES:

If Service Provider fails to deliver and perform any or all the Services within the stipulated time, schedule as specified in this RFP/Agreement, the Bank may, without prejudice to its other remedies under the RFP/Agreement, and unless otherwise extension of time is agreed upon without the application of liquidated damages, deduct from the Project Cost, as liquidated damages a sum equivalent to 0.5% of total Project Cost for delay of each week or part thereof maximum up to 5% of total Project Cost. Once the maximum deduction is reached, the Bank may consider termination of the Agreement.

41. CONFLICT OF INTEREST:

i. Bidder shall not have a conflict of interest (the "Conflict of Interest") that affects the bidding Process. Any Bidder found to have a Conflict of Interest shall be disqualified. In the event of disqualification, the Bank shall be entitled to forfeit and appropriate the Bid Security and/or Performance Security (Bank Guarantee), as the case may be, as mutually agreed upon genuine estimated loss and damage likely to be suffered and incurred by the Bank and not by way of penalty for, inter alia, the time, cost and effort of the Bank, including consideration of such Bidder's proposal (the "Damages"), without prejudice to any other right or remedy that may be available to the Bank under the bidding Documents and/ or the Agreement or otherwise.

ii. Without limiting the generality of the above, a Bidder shall be deemed to have a Conflict of Interest affecting the bidding Process, if:

(a) the Bidder, its Member or Associate (or any constituent thereof) and any other Bidder, its Member or any Associate thereof (or any constituent thereof) have common controlling shareholders or other ownership interest; provided that this disqualification shall not apply in cases where the direct or indirect shareholding of a Bidder, its Member or an Associate thereof (or any shareholder thereof having a shareholding of more than 5% (five per cent) of the paid up and subscribed share capital of such Bidder, Member or Associate, as the case may be) in the other Bidder, its Member or Associate, has less than 5% (five per cent) of the subscribed and paid up equity share capital thereof; provided further that this disqualification shall not apply to any ownership by a bank, insurance company, pension fund or a public financial institution referred to in section 2(72) of the Companies Act, 2013. For the purposes of this Clause, indirect shareholding held through one or more intermediate persons shall be computed as follows: (aa) where any intermediary is controlled by a person through

management control or otherwise, the entire shareholding held by such controlled intermediary in any other person (the "Subject Person") shall be taken into account for computing the shareholding of such controlling person in the Subject Person; and (bb) subject always to sub-clause (aa) above, where a person does not exercise control over an intermediary, which has shareholding in the Subject Person, the computation of indirect shareholding of such person in the Subject Person shall be undertaken on a proportionate basis; provided, however, that no such shareholding shall be reckoned under this sub-clause (bb) if the shareholding of such person in the intermediary is less than 26% of the subscribed and paid up equity shareholding of such intermediary; or

(b) a constituent of such Bidder is also a constituent of another Bidder; or

(c) such Bidder, its Member or any Associate thereof receives or has received any direct or indirect subsidy, grant, concessional loan or subordinated debt from any other Bidder, its Member or Associate, or has provided any such subsidy, grant, concessional loan or subordinated debt to any other Bidder, its Member or any Associate thereof; or

(d) such Bidder has the same legal representative for purposes of this Bid as any other Bidder; or

(e) such Bidder, or any Associate thereof, has a relationship with another Bidder, or any Associate thereof, directly or through common third party/ parties, that puts either or both of them in a position to have access to each other's information about, or to influence the Bid of either or each other; or

(f) Such Bidder or any of its affiliates thereof has participated as a consultant to the Bank in the preparation of any documents, design or technical specifications of the RFP.

iii. For the purposes of this RFP, Associate means, in relation to the Bidder, a person who controls, is controlled by, or is under the common control with such Bidder (the "Associate"). As used in this definition, the expression "control" means, with respect to a person which is a company or corporation, the ownership, directly or indirectly, of more than 50% (fifty per cent) of the voting shares of such person, and with respect to a person which is not a company or corporation, the power to direct the management and policies of such person by operation of law or by contract.

42. CODE OF INTEGRITY AND DEBARMENT/BANNING:

i. The Bidder and their respective officers, employees, agents and advisers shall observe the highest standard of ethics during the bidding Process. Notwithstanding anything to the contrary contained herein, the Bank shall reject Bid without being liable in any manner whatsoever to the Bidder if it determines that the Bidder has,

directly or indirectly or through an agent, engaged in corrupt/fraudulent/coercive/undesirable or restrictive practices in the bidding Process.

ii. Bidders are obliged under code of integrity to Suo-moto proactively declare any conflicts of interest (pre-existing or as and as soon as these arise at any stage) in RFP process or execution of contract. Failure to do so would amount to violation of this code of integrity.

iii. Any Bidder needs to declare any previous transgressions of such a code of integrity with any entity in any country during the last three years or of being debarred by any other procuring entity. Failure to do so would amount to violation of this code of integrity

iv. For the purposes of this clause, the following terms shall have the meaning hereinafter, respectively assigned to them:

(a) "**corrupt practice**" means making offers, solicitation or acceptance of bribe, rewards or gifts or any material benefit, in exchange for an unfair advantage in the procurement process or to otherwise influence the procurement process or contract execution;

(b) **"Fraudulent practice"** means any omission or misrepresentation that may mislead or attempt to mislead so that financial or other benefits may be obtained, or an obligation avoided. This includes making false declaration or providing false information for participation in an RFP process or to secure a contract or in execution of the contract;

(c) **"Coercive practice"** means harming or threatening to harm, persons or their property to influence their participation in the procurement process or affect the execution of a contract;

(d) **"Anti-competitive practice"** means any collusion, bid rigging or anti-competitive arrangement, or any other practice coming under the purview of the Competition Act, 2002, between two or more bidders, with or without the knowledge of the Bank, that may impair the transparency, fairness and the progress of the procurement process or to establish bid prices at artificial, non-competitive levels;

(e) **"Obstructive practice"** means materially impede the Bank's or Government agencies investigation into allegations of one or more of the above mentioned prohibited practices either by deliberately destroying, falsifying, altering; or by concealing of evidence material to the investigation; or by making false

statements to investigators and/or by threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation; or by impeding the Bank's rights of audit or access to information;

v. **Debarment/Banning**

Empanelment/participation of Bidders and their eligibility to participate in the Bank's procurements is subject to compliance with code of integrity and performance in contracts as per terms and conditions of contracts. Following grades of debarment from empanelment/participation in the Bank's procurement process shall be considered against delinquent Vendors/Bidders:

(a) **Holiday Listing (Temporary Debarment - suspension):**

Whenever a Vendor is found lacking in performance, in case of less frequent and less serious misdemeanors, the vendors may be put on a holiday listing (temporary debarment) for a period up to 12 (twelve) months. When a Vendor is on the holiday listing, he is neither invited to bid nor are his bids considered for evaluation during the period of the holiday. The Vendor is, however, not removed from the list of empaneled vendors, if any. Performance issues which may justify holiday listing of the Vendor are:

- Vendors who have not responded to requests for quotation/tenders consecutively three times without furnishing valid reasons, if mandated in the empanelment contract (if applicable);
- Repeated non-performance or performance below specified standards (including after sales services and maintenance services etc.);
- Vendors undergoing process for removal from empanelment/participation in procurement process or banning/debarment may also be put on a holiday listing during such proceedings.

(b) Debarment from participation including removal from empanelled list

Debarment of a delinquent Vendor (including their related entities) for a period (one to two years) from the Bank's procurements including removal from empanelment, wherever such Vendor is empaneled, due to severe deficiencies in performance or other serious transgressions. Reasons which may justify debarment and/or removal of the Vendor from the list of empaneled vendors are:

- Without prejudice to the rights of the Bank under Clause *39(i)* hereinabove, if a Bidder is found by the Bank to have directly or indirectly or through an agent, engaged or indulged in any corrupt/fraudulent/coercive/undesirable or restrictive practices during the bidding Process, such Bidder shall not be eligible to

participate in any EOI/RFP issued by the Bank during a period of 2 (two) years from the date of debarment.

- Vendor fails to abide by the terms and conditions or to maintain the required technical/operational staff/equipment or there is change in its production/service line affecting its performance adversely, or fails to cooperate or qualify in the review for empanelment;
- If Vendor ceases to exist or ceases to operate in the category of requirements for which it is empaneled;
- Bankruptcy or insolvency on the part of the vendor as declared by a court of law; or
- Banning by Ministry/Department or any other Government agency;
- Other than in situations of force majeure, technically qualified Bidder withdraws from the procurement process or after being declared as successful bidder: (i) withdraws from the process; (ii) fails to enter into a Contract; or (iii) fails to provide performance guarantee or any other document or security required in terms of the RFP documents;
- If the Central Bureau of Investigation/CVC/C&AG or Vigilance Department of the Bank or any other investigating agency recommends such a course in respect of a case under investigation;
- Employs a Government servant or the Bank's Officer within two years of his retirement, who has had business dealings with him in an official capacity before retirement; or
- Any other ground, based on which the Bank considers, that continuation of Contract is not in public interest.
- If there is strong justification for believing that the partners/directors/proprietor/agents of the firm/company have been guilty of violation of the code of integrity or Integrity Pact (wherever applicable), evasion or habitual default in payment of any tax levied by law etc.

(c) **Banning from Ministry/Country-wide procurements**

For serious transgression of code of integrity, a delinquent Vendor (including their related entities) may be banned/debarred from participation in a procurement process of the Bank including procurement process of any procuring entity of Government of India for a period not exceeding three years commencing from the date of debarment.

43. TERMINATION FOR DEFAULT:

i. The Bank may, without prejudice to any other remedy for breach of Agreement, written notice of not less than 30 (thirty) days, terminate the Agreement in whole or in part:
   (a) If Service Provider fails to deliver any or all the obligations within the time period specified in the RFP/Agreement, or any extension thereof granted by the Bank;
   (b) If Service Provider fails to perform any other obligation(s) under the RFP/Agreement;
   (c) Violations of any terms and conditions stipulated in the RFP;
   (d) On happening of any termination event mentioned in the RFP/Agreement.

   Prior to providing a written notice of termination to Service Provider under clause *40 (i) (a) to 40 (i) (c),* the Bank shall provide Service Provider with a written notice of 30 (thirty) days to cure such breach of the Agreement. If the breach continues or remains unrectified after expiry of cure period, the Bank shall have right to initiate action in accordance with above clause.

ii. In the event the Bank terminates the Contract in whole or in part for the breaches attributable to Service Provider, the Bank may procure, upon such terms and in such manner as it deems appropriate, Services similar to those undelivered, and subject to limitation of liability clause of this RFP Service Provider shall be liable to the Bank for any increase in cost for such similar Services. However, Service Provider shall continue performance of the Contract to the extent not terminated.

iii. If the Contract is terminated under any termination clause, Service Provider shall handover all documents/ executable/ Bank's data or any other relevant information to the Bank in timely manner and in proper format as per scope of this RFP and shall also support the orderly transition to another vendor or to the Bank.

iv. During the transition, Service Provider shall also support the Bank on technical queries/support on process implementation.

v. The Bank's right to terminate the Contract will be in addition to the penalties / liquidated damages and other actions as specified in this RFP.

vi. In the event of failure of Service Provider to render the Services or in the event of termination of Agreement or expiry of term or otherwise, without prejudice to any other right, the Bank at its sole discretion may make alternate arrangement for getting the Services contracted with another vendor. In such case, the Bank shall give prior notice to the existing Service Provider. The existing Service Provider shall continue to provide services as per the terms of the Agreement until a 'New

Service Provider' completely takes over the work. During the transition phase, the existing Service Provider shall render all reasonable assistance to the new Service Provider within such period prescribed by the Bank, at no extra cost to the Bank, for ensuring smooth switch over and continuity of services, provided where transition services are required by the Bank or New Service Provider beyond the term of this Agreement, reasons for which are not attributable to Service Provider, payment shall be made to Service Provider for such additional period on the same rates and payment terms as specified in this Agreement. If existing Service Provider is breach of this obligation, they shall be liable for paying a penalty of 10% of the total Project Cost on demand to the Bank, which may be settled from the payment of invoices or Bank Guarantee for the contracted period or by invocation of Bank Guarantee.

44. FORCE MAJEURE:

i. Notwithstanding the provisions of terms and conditions contained in this RFP, neither party shall be liable for any delay in in performing its obligations herein if and to the extent that such delay is the result of an event of Force Majeure.

ii. For the purposes of this clause, 'Force Majeure' means and includes wars, insurrections, revolution, civil disturbance, riots, terrorist acts, public strikes, hartal, bundh, fires, floods, epidemic, quarantine restrictions, freight embargoes, declared general strikes in relevant industries, Vis Major, acts of Government in their sovereign capacity, impeding reasonable performance of Service Provider and / or Sub-Contractor but does not include any foreseeable events, commercial considerations or those involving fault or negligence on the part of the party claiming Force Majeure.

iii. If a Force Majeure situation arises, Service Provider shall promptly notify the Bank in writing of such condition and the cause thereof. Unless otherwise directed by the Bank in writing, Service Provider shall continue to perform its obligations under the Contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

iv. If the Force Majeure situation continues beyond 30 (thirty) days, either party shall have the right to terminate the Agreement by giving a notice to the other party. Neither party shall have any penal liability to the other in respect of the termination of the Agreement as a result of an event of Force Majeure. However, Service Provider shall be entitled to receive payments for all services actually rendered up to the date of the termination of the Agreement.

45. TERMINATION FOR INSOLVENCY:

The Bank may, at any time, terminate the Contract by giving written notice to Service Provider, if Service Provider becomes Bankrupt or insolvent or any application for bankruptcy, insolvency or winding up has been filed against it by any person. In this event, termination will be without compensation to Service Provider, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to the Bank.

46. TERMINATION FOR CONVENIENCE:

i. The Bank, by written notice of not less than 90 (ninety) days, may terminate the Contract, in whole or in part, for its convenience, provided same shall not be invoked by the Bank before completion of half of the total Contract period (including the notice period).

ii. In the event of termination of the Agreement for the Bank's convenience, Service Provider shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.

47. DISPUTES / ARBITRATION (APPLICABLE IN CASE OF SUCCESSFUL BIDDER ONLY):

i. All disputes or differences whatsoever arising between the parties out of or in connection with the Contract (including dispute concerning interpretation) or in discharge of any obligation arising out of the Contract (whether during the progress of work or after completion of such work and whether before or after the termination of the Contract, abandonment or breach of the Contract), shall be settled amicably. If however, the parties are not able to solve them amicably within 30 (thirty) days after dispute occurs as evidenced through the first written communication from any Party notifying the other regarding the disputes, either party (SBI or Service Provider), give written notice to other party clearly setting out there in specific dispute(s) and/or difference(s) and shall be referred to a sole arbitrator mutually agreed upon, and the award made in pursuance thereof shall be binding on the parties. In the absence of consensus about the single arbitrator, the dispute may be referred to an arbitration panel; one to be nominated by each party and the said arbitrators shall nominate a presiding arbitrator, before commencing the arbitration proceedings. The arbitration shall be settled in accordance with the applicable Indian Laws and arbitration proceeding shall be conducted in accordance with Arbitration and Conciliation Act 1996 and any amendment thereto. Any appeal will be subject to the exclusive jurisdiction of courts at Mumbai.

ii. Service Provider shall continue work under the Contract during the arbitration proceedings unless otherwise directed by the Bank or unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator is

obtained.

iii. Arbitration proceeding shall be held at Mumbai, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be in English.

48. GOVERNING LANGUAGE:

The governing language shall be English.

49. APPLICABLE LAW:

The Contract shall be interpreted in accordance with the laws of the Union of India and shall be subjected to the exclusive jurisdiction of courts at Mumbai.

50. TAXES AND DUTIES:

i. Service Provider shall be liable to pay all corporate taxes and income tax that shall be levied according to the laws and regulations applicable from time to time in India and the price Bid by Service Provider shall include all such taxes in the quoted price.

ii. Prices quoted should be exclusive of all Central / State Government taxes/duties and levies but inclusive of all corporate taxes and Custom duty as also cost of incidental services such as transportation, road permits, insurance etc. The quoted prices and taxes/duties and statutory levies such as GST etc. should be specified in the separate sheet **(Appendix- F).**

iii. Custom duty as also cost of incidental services such as transportation, road permits, insurance etc. in connection with delivery of products at site including any incidental services and commissioning, if any, which may be levied, shall be borne by Service Provider and the Bank shall not be liable for the same. Only specified taxes/ levies and duties in the **Appendix-F** will be payable by the Bank on actuals upon production of original receipt wherever required. If any specified taxes/ levies and duties in **Appendix-F** are replaced by the new legislation of Government, same shall be borne by the Bank. The Bank shall not be liable for payment of those Central / State Government taxes, levies, duties or any tax/ duties imposed by local bodies/ authorities, which are not specified by the Bidder in **Appendix-F**

iv. Prices payable to Service Provider as stated in the Contract shall be firm and not subject to adjustment during performance of the Contract, irrespective of reasons whatsoever, including exchange rate fluctuations, any upward revision in Custom duty.

v. Income / Corporate Taxes in India: The Bidder shall be liable to pay all corporate taxes and income tax that shall be levied according to the laws and regulations applicable from time to time in India and the price Bid by the Bidder shall include all such taxes in the contract price.

vi. All expenses, stamp duty and other charges/ expenses in connection with the execution of the Agreement as a result of this RFP process shall be borne by Service Provider. The Agreement/ Contract would be stamped as per Maharashtra Stamp Act, 1958 and any amendment thereto.

51. TAX DEDUCTION AT SOURCE:

i. Wherever the laws and regulations require deduction of such taxes at the source of payment, the Bank shall effect such deductions from the payment due to Service Provider. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by the Bank as per the laws and regulations for the time being in force. Nothing in the Contract shall relieve Service Provider from his responsibility to pay any tax that may be levied in India on income and profits made by Service Provider in respect of this Contract.

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

52. TENDER FEE:

Non-refundable Tender Fee should be directly credited to the designated account as mentioned in Schedule of Events. Proof of remittance of Tender Fee in the designated account should be enclosed with the technical bid. The Bids without tender fee will not be considered valid.

53. EXEMPTION OF EMD AND TENDER FEE:

Micro & Small Enterprises (MSE) units and Start-ups* are exempted from payment of tender fee and tender fee provided the Services they are offering, are rendered by them. Exemption as stated above is not applicable for providing services, rendered by other companies.

Bidder should submit supporting documents issued by competent Govt. bodies to become eligible for the above exemption.

Bidders may please note:

i. NSIC certificate/ Udyog Aadhar Memorandum/ Udyam Registration Certificate should cover the items tendered to get tender fee exemptions. Certificate/ Memorandum should be valid as on due date / extended due date for Bid submission.

ii. "Start-up" company should enclose the valid Certificate of Recognition issued by Department for Promotion of Industry and Internal Trade (DPIIT), (erstwhile Department of Industrial Policy and Promotion), Ministry of Commerce & Industry, Govt. of India with the technical bid.

iii. *Start-ups which are not under the category of MSE shall not be eligible for exemption of tender fee.

iv. Bidder who solely on its own, fulfils each eligibility criteria condition as per the RFP terms and conditions and who are having MSE or Start-up company status, can claim exemption for tender fee.

v. If all these conditions are not fulfilled or supporting documents are not submitted with the technical Bid, then all those Bids without tender fees will be summarily rejected and no queries will be entertained.

54. NOTICES:

Any notice given by one party to the other pursuant to this Contract shall be sent to other party in writing or by Fax and confirmed in writing to other Party's address. The notice shall be effective when delivered or on the notice's effective date whichever is later.

Part-II

Appendix –A

BID FORM (TECHNICAL BID)

[On Company's letter head]

(To be included in Technical Bid)

Date: _____

To:

Deputy General Manager
Platform Engineering-I Department,
State Bank of India Global IT Centre,
Gr Floor 'B'- Wing, Plot no 8/9/10,
Sector -11, CBD Belapur
Navi Mumbai- 400614

Madam /Dear Sir,

Ref: RFP No. SBI/GITC/Platform Engineering-I/2021/2022/809 Dated: 06-Dec-2021

We have examined the above RFP, the receipt of which is hereby duly acknowledged and subsequent pre-bid clarifications/ modifications / revisions, if any, furnished by the Bank and we offer to provide Services detailed in this RFP. We shall abide by the terms and conditions spelt out in the RFP. We shall participate and submit the commercial Bid through online auction to be conducted by the Bank's authorized service provider, on the date advised to us.

i. While submitting this Bid, we certify that:
   - The undersigned is authorized to sign on behalf of the Bidder and the necessary support document delegating this authority is enclosed to this letter.
   - We declare that we are not in contravention of conflict of interest obligation mentioned in this RFP.
   - Indicative prices submitted by us have been arrived at without agreement with any other Bidder of this RFP for the purpose of restricting competition.
   - The indicative prices submitted by us have not been disclosed and will not be disclosed to any other Bidder responding to this RFP.
   - We have not induced or attempted to induce any other Bidder to submit or not to submit a Bid for restricting competition.

- We have quoted for all the services/items mentioned in this RFP in our indicative price Bid.
- The rate quoted in the indicative price Bids are as per the RFP and subsequent pre-Bid clarifications/ modifications/ revisions furnished by the Bank, without any exception.

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

iii. We undertake that we will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Bank, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

iv. We undertake that we will not resort to canvassing with any official of the Bank, connected directly or indirectly with the bidding process to derive any undue advantage. We also understand that any violation in this regard, will result in disqualification of bidder from further bidding process.

v. It is further certified that the contents of our Bid are factually correct. We have not sought any deviation to the terms and conditions of the RFP. We also accept that in the event of any information / data / particulars proving to be incorrect, the Bank will have right to disqualify us from the RFP without prejudice to any other rights available to the Bank.

vi. We certify that while submitting our Bid document, we have not made any changes in the contents of the RFP document, read with its amendments/clarifications provided by the Bank.

vii. We agree to abide by all the RFP terms and conditions, contents of Service Level Agreement as per template available at **Appendix-J** of this RFP and the rates quoted therein for the orders awarded by the Bank up to the period prescribed in the RFP, which shall remain binding upon us.

viii. On acceptance of our technical bid, we undertake to participate in Reverse auction by way of login in Reverse auction tool. In case of declaration as successful Bidder on completion of Reverse auction process, we undertake to complete the formalities as specified in this RFP.

ix. The commercial bidding process will be through the reverse auction process to be conducted by the Bank or a company authorized by the Bank. We understand that our

authorized representative who would participate in the reverse auction process would be possessing a valid digital certificate for the purpose.

x. Till execution of a formal contract, the RFP, along with the Bank's notification of award by way of issuance of purchase order and our acceptance thereof, would be binding contractual obligation on the Bank and us.

xi. We understand that you are not bound to accept the lowest or any Bid you may receive, and you may reject all or any Bid without assigning any reason or giving any explanation whatsoever.

xii. We hereby certify that our name does not appear in any "Caution" list of RBI / IBA or any other regulatory body for outsourcing activity.

xiii. We hereby certify that on the date of submission of Bid for this RFP, we do not have any past/ present litigation which adversely affect our participation in this RFP or we are not under any debarment/blacklist period for breach of contract/fraud/corrupt practices by any Scheduled Commercial Bank/ Public Sector Undertaking/ State or Central Government or their agencies/departments.

xiv. We hereby certify that on the date of submission of Bid, we do not have any Service Level Agreement pending to be signed with the Bank for more than 6 months from the date of issue of purchase order.

xv. We hereby certify that we have read the clauses 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 regarding restrictions on procurement from a bidder of a country which shares a land border with India. We further certify that we and our OEM are not from such a country or if from a country, has been registered with competent authority. We certify that we and our OEM fulfil all the requirements in this regard and are eligible to participate in this RFP.

xvi. If our Bid 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 and we shall be solely responsible for the due performance of the contract.

xvii. We understand that as per clause 9 of the RFP, Bids must be supported by a Bid Security Declaration in lieu of EMD. Accordingly, we furnish this Bid Security Declaration and undertake that (a) we shall not withdraw or modify our bid during the period of Bid validity; (b) if we are considered technically qualified Bidder by the Bank, we shall participate in the auction by logging in, in the reverse auction tool; (c) we have not made any statement or enclosed any form which may turn out to be false/ incorrect at any time prior to signing of Contract; (d) if we are awarded the Contract, we shall accept Purchase

Order and/or sign the Contract with the Bank and furnish Bank Guarantee, within the specified time period in the RFP.

xviii. We, further, hereby undertake and agree to abide by all the terms and conditions stipulated by the Bank in the RFP document.

Dated this ..... day of 201

_____

(Signature) *(Name)*

(In the capacity of)

Duly authorized to sign Bid for and on behalf of

_____**Seal of the company.**

Appendix-B

Bidder's Eligibility Criteria

Bidders meeting the following criteria are eligible to submit their Bids along with supporting documents. If the Bid is not accompanied by all the required documents supporting eligibility criteria, the same would be rejected:

S. No.	Eligibility Criteria	Compliance (Yes/No)	Documents to be submitted
1.	The Bidder must be an Indian Company/ LLP /Partnership firm registered under applicable Act in India.		Certificate of Incorporation issued by Registrar of Companies and full address of the registered office along with Memorandum & Articles of Association/ Partnership Deed.
2.	The Bidder (including its OEM, if any) 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 specifically certify in **Appendix A** in this regard and provide copy of registration certificate issued by competent authority wherever applicable.
3.	The Bidder must have an average turnover of minimum Rs. **185** crore during last 03 (three) financial year(s) i.e. FY 2017-18, FY 2018-19 and FY 2019-20.		Copy of the audited financial statement for required financial years. (Certificate from statutory auditor for preceding/current 03 year to be submitted.)
4.	The Bidder should be profitable organization on the basis of profit before tax (PBT) for at least 02 (two) out of last 03 (three) financial years mentioned in para 3 above.		Copy of the audited financial statement along with profit and loss statement for corresponding years and / or Certificate of the statutory auditor.
5.	Bidder should have experience of minimum **03** years in providing the "EPP, ACC and FIM" for large deployments in any organization for at least one lakh Endpoints in a single installation for top verifiable Indian / Blue-chip /Fortune 500 / BFSI / Service Sector company preferable in India. Global verifiable references will also be		Copy of the purchase order and Certificate of completion of the work from reputed clients to be submitted. The Bidder should also furnish user acceptance report. The documents should clearly establish the required period of experience.

	considered. For single installation the principal organization will only be considered excluding its subsidiaries/associates.		
6	Bidder should have experience of minimum **02** years in providing the "EDR" for large deployments in any organization for at least 25,000 Endpoints in a single installation for top Indian / Blue-chip /Fortune 500 / BFSI / Service Sector company preferable in India. Global verifiable references will also be considered. For single installation the principal organization will only be considered excluding its subsidiaries/associates.		Copy of the purchase order and Certificate of completion of the work from reputed clients to be submitted. The Bidder should also furnish user acceptance report. The documents should clearly establish the required period of experience. All references provided should be verifiable by the Bank.
7.	Proposed OEM solution (for EPP, ACC & EDR) should be successfully running for at least 50,000 Endpoints (i.e. desktops), in a single installation, since minimum three years for top Indian / Blue-chip /Fortune 500 / BFSI / Service Sector companies in India. Global verifiable references will also be considered. For single installation the principal organization will only be considered excluding its subsidiaries/associates.		Copy of purchase order and Certificate of completion of the work from reputed clients to be submitted. The Bidder should also furnish user acceptance report. The documents should clearly establish the required period of experience. All references provided should be verifiable by the Bank.
8.	Proposed OEM solution (EPP, ACC, FIM & EDR) should be successfully running for at least 5,000 servers, in a single installation, since minimum three years for top Indian / Blue-chip /Fortune 500 / BFSI / Service Sector companies in India. Global verifiable references will also be considered For single installation the principal organization will only be considered excluding its subsidiaries/associates.		Copy of purchase order and Certificate of completion of the work from reputed clients to be submitted. The Bidder should also furnish user acceptance report. The documents should clearly establish the required period of experience. All references provided should be verifiable by the Bank.
9.	Verifiable Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects.		Bidder should specifically confirm on their letter head in this regard as per **Appendix-M**

	(Start date and End Date of the Project to be mentioned) in the past (not less than 02 client references are required).		Bank will make 2 attempts to verify customer references through email/call within a total period of 7 days after first email/call. If, the customer response is not received within 7 days of first email/call, the customer reference will be treated as non-responsive, and bid will be rejected. The bidder will be solely responsible for such rejection.
10.	Certification Requirements: I. A certificate from CEO/CISO of the OEM to be submitted confirming that the proposed ESS solution is fully secured for deployment in SBI. II. The proposed solution should be ISO-27001 & ISO 27017 or Global SOC2 certified.		I. Copy of the certificate from OEM on company letterhead at the time of bidding as per Appendix-O. II. A copy of the ISO-27001 & ISO 27017 or Global SOC2 valid certificate indicating its validity. A declaration should also be submitted that these certificates will be valid during the contact period with Bank under this RFP.
11.	Past/present litigations, disputes, if any (Adverse litigations could result in disqualification, at the sole discretion of the Bank)		Brief details of litigations, disputes related to product/services being procured under this RFP or infringement of any third party Intellectual Property Rights by prospective Bidder/ OEM or disputes among Bidder's board of directors, liquidation, bankruptcy, insolvency cases or cases for debarment/blacklisting for breach of contract/fraud/corrupt practices by any Scheduled Commercial Bank/ Public Sector Undertaking / State or Central Government or their agencies/

			departments or any such similar cases, if any are to be given on Company's letter head.
12.	Bidders should not be under debarment/blacklist period for breach of contract/fraud/corrupt practices by any Scheduled Commercial Bank/ Public Sector Undertaking / State or Central Government or their agencies/ departments on the date of submission of bid for this RFP.		Bidder should specifically certify in **Appendix A** in this regard.
13.	The Bidder should not have any Service Level Agreement pending to be signed with the Bank for more than 6 months from the date of issue of purchase order.		Bidder should specifically certify in **Appendix A** in this regard.
14.	The proposed OEM and their existing cloud Partner (if any) should be empaneled with MeiTY as on RFP release date.		MeiTY Empanelment Certificate in the name of proposed OEM / existing cloud partner to be submitted.
15.	The Bidder should be one of the highest rated authorized partners of the OEM as per their assessment criteria on the date of issue of RFP.		Confirmation on OEM letter head for the Bidder to be submitted.
16.	OEM's and its Cloud Service Provider's (CSP) data centers should be minimum Rated 3 of TIA940 or Tier 3 of 'Uptime Institute' or any other equivalent certification.		Relevant certificates to be submitted.

Documentary evidence must be furnished against each of the above criteria along with an index. All documents must be signed by the authorized signatory of the Bidder. Relevant portions, in the documents submitted in pursuance of eligibility criteria, should be highlighted.

Eligibility criteria mentioned at Sl No 2 to 4 in table above are relaxed for Startups subject to their meeting of quality and technical specifications. Bidder to note the followings:

i. Start-up" company should enclose the valid Certificate of Recognition issued by Department for Promotion of Industry and Internal Trade (DPIIT), (erstwhile Department of Industrial Policy and Promotion), Ministry of Commerce & Industry, Govt. of India with the technical bid.

ii. Bidder who solely on its own, fulfils each eligibility criteria condition as per the RFP terms and conditions and who are having Start-up company status, can claim exemption for eligibility criteria mentioned at Sl No 2 to 4 in table above.

iii. If all these conditions are not fulfilled or supporting documents are not submitted with the technical Bid, then all those Bids will be summarily rejected, and no queries will be entertained.

Name & Signature of authorized signatory
Seal of Company

Appendix-B1

SECURITY CONTROLS

In addition to the eligibility criteria defined in Appendix-B, Bidder and OEM both are also required to comply with the following points and submit compliance of the same on their letter head along with the relevant certificates, to the Bank along with bid documents. In case bidder and OEM are not same, a back-to-back confirmation from OEM should also be submitted for compliance to these security controls on OEM letter head. In case of non-compliance of any of the requirement, Bid would be rejected:
(Please Note, while submitting compliance of below controls by OEM, the word Bidder Should be replaced by OEM)

S. No.	Required Controls	Compliance (Yes/No)
1	Whether Bidder has information security policy in place with periodic review	
2	Whether Bidder has operational processes with periodic review, including but not limited to: a) Business continuity management b) Backup Management c) Desktop/ system/ server/ network device hardening with baseline controls d) Patch management e) Port management f) Media movement g) Log management h) Personnel security i) Physical security j) Internal security assessment processes	
3	Whether Bidder has instituted proper documented change management process.	
4	Whether Bidder has proper documented policy and process of incident management/ response.	
5	Whether Bidder IT environment is suitably protected from external threats by way of firewall, WAF, IDS/IPS, AD, AV, NAC, DLP, NTP.	
6	Whether Bidder has approved process for implementing rules on firewalls in its environment and the same are followed.	
7	Whether Bidder monitors firewall rule position regularly for presence of any vulnerable open port or any-any rule.	

8	Whether Bidder has captive SOC or managed service SOC for monitoring their system and operations.	
9	Whether Bidder environment is segregated into militarized zone (MZ) and demilitarized zone (DMZ) separated by firewall, where any access from an external entity is permitted through DMZ only.	
10	Whether Bidder has deployed secure production, disaster recovery and testing environment for their application.	
11	Bidder to confirm that no internet access is permitted on internal servers, database servers.	
12	Whether the Bidder has a dedicated information security team independent of IT, reporting directly to MD/CIO for conducting security related functions & operations.	
13	Bidder will engage CERT-IN Empaneled ISSPs for ensuring security posture of their application.	
14	Whether quarterly vulnerability assessment and penetration testing is being done by the Bidder for their IT infrastructure.	
15	Whether suitable security certification (ISO, PCI-DSS) of the security posture at Bidder IT environment are in place.	
16	While sharing the data, whether Bidder is agreeable to encrypt the same as per industry best standards with robust key management.	
17	Whether Bidder is agreeable to completely erase the data after processing at their end, if so permitted to be stored.	
18	Whether Bidder is agreeable to store the data with encryption (Data at rest encryption), if storing is permitted in RFP.	
19	Whether Bidder is agreeable to get the data storage technology (Servers /Public Cloud/ Tapes) appropriately reviewed by the Bank.	
20	Bidder to confirm that it will not share the Bank's data to any other party for any purpose without prior permission of the Bank.	
21	Whether Bidder is willing to put in place a system of obtaining approval from the Bank	

	before carrying out any changes in their environment.	
22	Bidder to confirm that it will not take any crucial decisions on behalf of the Bank without written approval from the Bank.	
23	Whether Bidder is willing to implement efficient and sufficient preventive controls to protect the Bank's interests against any damage under section 43 of IT Act.	
24	Whether Bidder is agreeable to provide the process by which segregation of user accounts, database, backup, application admin and support account activities is achieved.	
25	Whether the Bidder is agreeable to store the archived data in a manner that it will not be available over internet in any case and will have restricted access.	
26	If required by the Bank, whether the Bidder is willing to use Competent Authority (CA) approved digital signing for non-repudiation purpose.	
27	Whether Bidder is willing to purge the post archival data regularly and report the same to the Bank.	
28	Whether controls have been put in place for PKE keys, if stored locally for providing access to privileged user access only.	
29	In case of data leaving the Bank's premises for module/functionality available on Bidder cloud, should adhere to the existing Indian legislation, regulatory guidelines, and Bank's IT/IS Policy.	
30	Controls should be in place to ensure protection of secret or confidential information of the Bank, stored in cloud as per applicable legal and regulatory requirements according to Indian jurisdiction.	
31	Bidder has to ensure the Bank's approved SCDs are implemented on the Bidder cloud or alternately the Bidder hardening guides should be reviewed to ensure that Bank's data is treated at equal or better level of security.	
32	All communications related to "Endpoint Security Solution" feature hosted in the cloud should be encrypted.	

33	Telemetry data of the Bank collected by the bidder in their cloud should not have sensitive / critical data stored.	
34	The Bidder should note that all data belong to the Bank and that Bidder should have **no rights or licenses**, including without limitation intellectual property rights or licenses, to use the data for its own purposes by virtue of the transaction or claim any security interest in the Bank's data.	
35	Bank's data is prohibited from extraterritorial storage outside India's geography and jurisdiction.	
36	Bank has right to audit / review Bidder data centers and security policies, processes / infrastructure as and when demanded by the Bank.	
37	Bidder should ensure that that logging is implemented on its cloud so that it's forensic ready.	
38	All logs of the "Endpoint Security Solution" should be integrated with the Bank's SOC.	
39	On termination of contract with Bidder or Bank's decision to discontinue utilizing the services, the complete data belonging to Bank should be provided back to the Bank and erased from Bidder end.	
40	Proposed solution and Bidder cloud shall be configured, deployed and managed to meet security, privacy, legal, ethical and compliance requirements of the Bank	
41	Information security controls in respect of "Security of the Cloud" and the "Security in the Cloud" must be at least as robust as those which the Bank would have implemented had the operations been performed in-house.	
42	Bidder must ensure that the Bank's data in their cloud or any Cloud Service Provider (CSP) engaged by them is prohibited from extra-territorial storage outside India's geography and jurisdiction	
43	Bidder should be empaneled with the Ministry of Electronics and Information Technology (MeiTY). In case bidder is using other cloud service provide then the designated CSP of the	

	Bidder should be empaneled with the Ministry of Electronics and Information Technology (MeiTY).	
44	Bidder cloud or its designated cloud service provider should be ISO-27001 & ISO-27017/ SOC2 compliant.	
45	Bidder data centers and their cloud service provider data centers CSP should be minimum Rated 3 of TIA940 or Tier 3 of Uptime Institute or any other equivalent certification. Additionally, Bidder or their cloud service provider should be ISO-27018 certified where PII/ SPDI data is involved.	
46	In case any credit card or debit card data is processed/stored or involved in any manner, the Bidder or their cloud service provider should be PCI-DSS compliant.	
47	Connectivity of ESS central management server deployed in Bank's premises with the Bidder cloud or their cloud service provider should be capable to have at least through two dedicated line i.e. (MPLS link) from two different telecom service provider through shortest route.	

Name & Signature of authorized signatory

Seal of Company

Appendix-C

Technical & Functional Specifications

In view of the advancements in Tactics, Techniques and Procedures (TTPs) used by the threat actors for committing cybercrimes, the Bank intends to procure a uniform Endpoint Security Solution (ESS) for deploying across the Bank. The salient features of the comprehensive ESS include but not limited to Endpoint Protection Platform (EPP), Application Change Control (ACC), File Integrity Monitoring (FIM) and Endpoint Detection and Response (EDR) as a comprehensive solution for STATE BANK GROUP termed as "Endpoint Security Solution (ESS)". The solution is proposed to be hosted as Hybrid Model i.e. Bank on-premises private cloud and with limited/minimum features through OEM's Datacenter, subject to compliance of Bank's latest as well as future versions of Information Security Policy and Guidelines and in compliance with the Regulatory and Legal framework mandated by various regulatory and government authorities of India from time to time.

Currently multiple agents are installed (viz. AV, ACC, FIM, EDR) on the endpoints which need to be consolidated into a single comprehensive solution with log collection and integration features for overall efficiency, manageability, comprehensive security posture visibility into the activities of endpoints, servers and roaming clients available in the Bank.

Expected key features in an Endpoint Security Solution (ESS):

1. The proposed central management server hosted in the Bank premises for Endpoint Security Solution should be able to monitor the up/down status, health and performance parameters and security posture of each service on the endpoints. In case the service is found to be down or underperforming than the baseline expectations, there should be a mechanism to automatically restart a particular service from the central manager.
2. All versions of agents on all the endpoints including desktops (Windows and non-Windows), Servers (Windows and non-Windows OS) On-premise and Off-premise Cloud setup, Virtual Machines, Mobile devices (iPad, tablets, Mobile phone, laptops any other endpoint.) and roaming/remote / standalone systems deployed of the Bank should be monitored / manageable through a single On-premise hosted orchestrator/management Server and console only.
3. The Endpoint Security Solution (ESS) agent shall consolidate the functionalities of multiple sub-agents running on the Bank's IT assets currently, like EPP/ACC/FIM/EDR so that single comprehensive solution can be deployed and the load on the endpoints system is reduced.
4. The solution should also provide the means to deploy the agents on all the assets/endpoints in one session and in one go as well as start its functioning / services on the Bank's assets remotely.
5. The Endpoint Security Solution (ESS) should be able to integrate with the Bank's existing NAC solution. The selected Bidder and OEM are responsible to provide end to end support in this regard.

6. The ESS should allow the Bank to dynamically cap the resource utilization (CPU/Memory) on the endpoints. The WAN bandwidth usage should be minimized especially during business hours of different offices.
7. The system should be able to provide both real-time scans (for new files and URLs) and scheduled scans (for scanning all the files against newly deployed signatures).
8. Protection from malicious web downloads: The ESS should analyze incoming and outgoing traffic and provide internet browser protection to block malicious web downloads before they are loaded into the RAM/Cache/Virtual memory of endpoints, as also before opened / executed on the endpoints.
9. Protection from exploits: This protects against zero-day vulnerabilities and memory-based attacks.
10. Application and device control: These enable organizations to control which systems can upload or download data, files, information, access firmware/kernel of hardware, software, applications access the registry. in the systems. It can reduce the chances of shadow IT with application allow lists or block lists, ensuring only approved software and apps are installed on endpoints.
11. Reports and alerts: These provide prioritized warnings and alerts regarding vulnerabilities, as well as dashboards and reports.
12. Detecting threats as early as possible is crucial: The longer a threat sits in the environment, the more it spreads and the more damage it can do. Real-time detection capabilities required.
13. Incident investigation and remediation: These include centralized and automated tools to provide automated incident response approaches and step-by-step workflows to investigate incidents.
14. Advanced Machine Learning based Behavior Anomaly detection and remediation: Analyzes massive amount of system events, tasks, processes, memory contents, good and bad files/data, vulnerabilities and virtual patching in all the systems across the Bank, correlate with internally generated IOCs and IOAs as also with global tactical and strategic intelligence (including IOCs and IOAs), zero day exploits and vulnerabilities and blocks new malware variants, old malwares with engineered / specially crafted for targeted attacks on the Bank before they infect the endpoints. This protection mechanism must be completely independent of signatures.
15. Third-party integrations: Endpoint Security Solution should communicate with other security systems in the Bank's on premise and off-premise IT environment. ESS should ingest / consume and also share threat intelligence with third party integrated systems in real-time mode leveraging API, Micro services mechanism as per Bank's decision. Using open API systems, ESS should integrate with other security tools, such as Active Directory, IDS, IPS, WAF, SOC, PIMS, NTP, NOC, Internet Proxy and with other those third-party systems which will be procured during the contract period.
16. Flexible deployment options: Endpoint Security Solution should adapt to the organization's needs and environment, offering on-premises, hybrid cloud or cloud deployment options from time to time as per Bank's discretion. Tool should also offer protection for every endpoint/server/roaming client that touches data.
17. Endpoint Security Solution Threat Intelligence: This includes web reputation of each URL and IP the Bank's internal system would attempt to connect. This check must be performed before the system connect to URL / IP and block the

communication if the web reputation of URL/IP and contents hosted or attempted for access by the Bank's internal system/endpoints is below the baselines standards defined as per best practices or by Bank.

18. Sandboxing: This is an isolated environment which to be deployed by the selected vendor to securely open / execute unknown or suspicious program/URL/contents to conduct comprehensive checking for any malicious content and its impact on the Bank's systems and stops their delivery into the endpoints.
19. Bank proposes to provide the virtual servers in its on-premises private cloud for deployment of central infrastructure servers of endpoint security solution. However, bidders are free to consider 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.

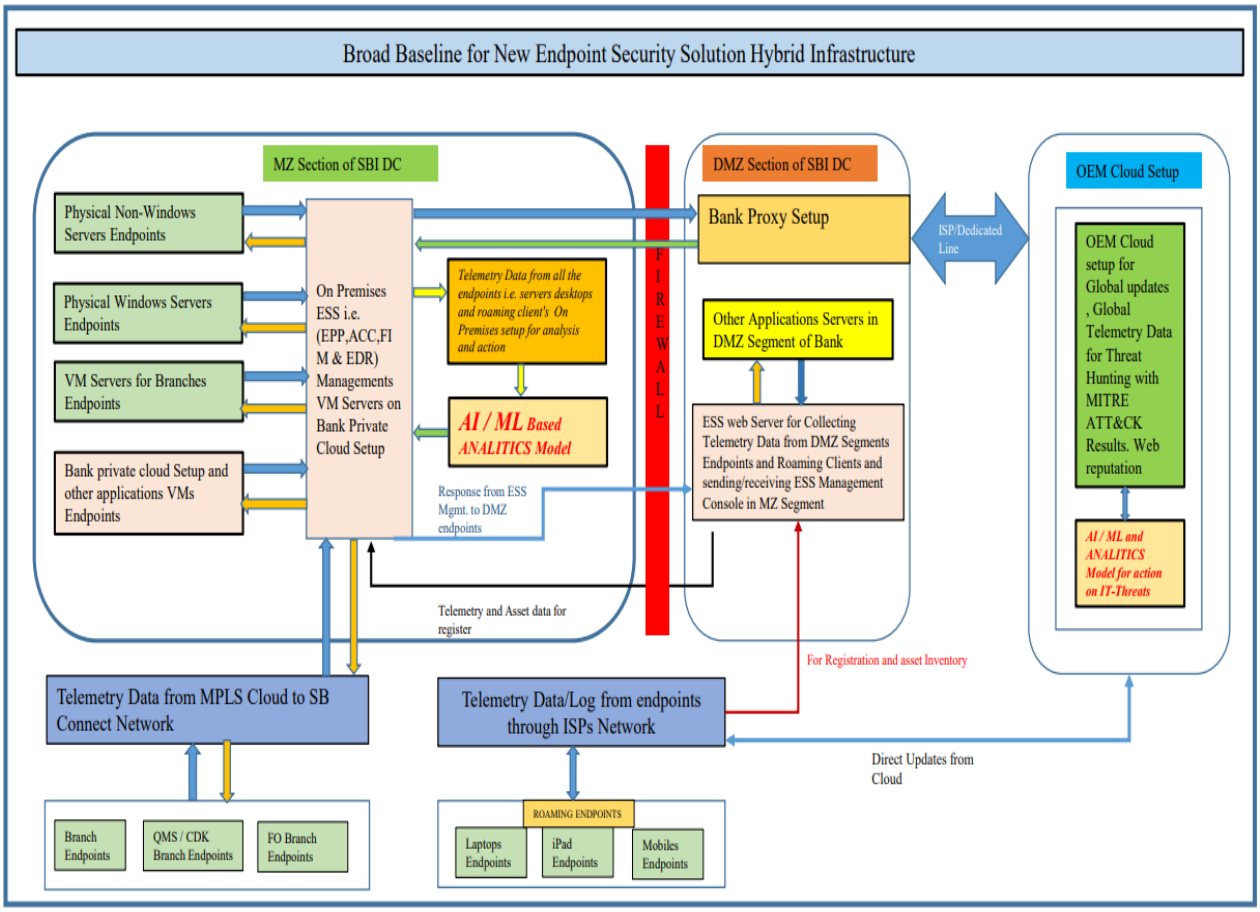
Hybrid Model - Definition and requirements:

Component	Parameters	Hybrid Model
Endpoint security solution Agents	Agent deployment	Agent will be installed on the endpoints.
	Update / Configuration changes on agents	1. Updates / Configuration changes from the Endpoint security solution central management server deployed in the Bank's Data Centre will be pushed to the agents on the endpoints (desktops, servers, remote devices). 2. Updates / Configuration changes from the Endpoint security solution deployed in service provider's Cloud will be pushed to the agents on the roaming clients external to Bank network over Internet.
Endpoint security solution Management Server	Deployment	This will be installed in the Bank's Data Centre in High Availability, both within and across Data Centers and DR site.
	Management access	The management / administrative access will be available from Bank's premises.
Endpoint security solution Threat Intelligence	Threat Detection and Analysis.	Endpoint security solution Threat Intelligence components may be deployed on Service Provider's Cloud.
	Web Reputation	Both the options are available.

Component	Parameters	Hybrid Model
Endpoint security solution Sandboxing	File and URL analysis and Data Privacy	File and URL analysis will be carried out on the Service Provider's Cloud. Sandboxing components shall be deployed on premise.

- Above proposed Hybrid Model is basic minimum requirement of the Bank. The Bidder has to provide proposed deployment architecture in the technical bid.
- No Endpoints will be connected with the OEM cloud directly, they will be connected with the central management server deployed in Bank premises which will in-turn be connected with the OEM cloud through Bank's proxy / dedicated link.
- Bidder/OEM cloud should not store and share Bank's sensitive/critical data stored. Bidder/OEM must ensure and provide evidence to prove that the all data / information / files /data. of that Bank shall be stored only on their India based servers and shall not be transported outside India to their or any other third party for any purpose.
- Threat detection and analysis will be carried out on the Service Provider's Cloud based on the information "**excluding"** (critical/sensitive information) gathered from the Bank's endpoints.
- File and URL analysis will be carried out on the Service Provider's Cloud if not available on premises.
- Latest signatures, IOCs, IOAs, AI/ML models and other Threat Intelligence Feeds can be fetched through SBI gateway/proxy/dedicated link connected to OEM cloud on to on-premises setup (Endpoint Security Solution Central Manager)
- Information/ application migrated to OEM's cloud should not have sensitive/ critical data (PII, SPDI, transaction level data).

Hybrid Model – Illustrative High-Level Architecture:



Above Hybrid model is High Level Diagram (HLD) for ESS solution. Bank required the dataflow from various endpoints to central ESS servers deployed in hybrid model are as under:

1. ESS agent available in SBI branch/admin office/FO branches/QMS/CDK systems will collect telemetry data and sent it to ESS central servers deployed in Bank Data center through MPLS link.
2. ESS agent available in roaming systems (i.e. laptop, iPad, Mobile) will collect telemetry data and sent it to ESS central servers deployed in Bank Data center DMZ segment through internet for logs and asset registration.
3. ESS central server will also receive telemetry data from physical server (windows & non-windows), BSC setup and VM servers in Meghdoot setup through data center LAN.
4. The telemetry data received by central ESS server will be analyze by using AI/ML models for appropriate response in case of any IT-threat.
5. ESS central servers in MZ and DMZ segment will receive regular update and other types of IT-Threat hunting information from OEM cloud through Banks proxy by using internet link or dedicated MPLS link.
6. Roaming clients will get the regular updates and remediation responses in case of any IT-Threat directly from the OEM cloud through internet link used by the user.
7. ESS central managements server deployed in Bank premises must pull the updates from OEM cloud.

8. ESS central managements server deployed in Bank premises must push the updates to the endpoints as and when the new update are available with ESS central manager.
9. Solution should collect the telemetry data from the endpoints and create IOA and IOC's.
10. The telemetry data collected from the endpoints should be stored for more than 3 months to analyzed the slow attacks (general APT's)
11. The ESS solution should be capable to share the telemetry or metadata of endpoints with OEM for correlation with JIT global telemetry.
12. Solution must be capable to fetch the OEM's global telemetry data also for correlation with local telemetry.
13. ESS solution must run AL/ML models preferable instead of signature base detection.
14. ESS solution should support ML models on ESS agents and keep regular updating these ML models.
15. OEM has to create SBI specific models for protection of the endpoints from IT and non-IT-Threats.
16. ESS solution architecture should be designed to collect Roaming client telemetry/logs also.
17. ESS solution should maintain at least 03-month logs online to analyze slow attack.
18. Proposed ESS solution should also support future readiness to detect/prevent newly invented IT threat as well as ESS feature and modular technology upgradation without any additional cost to the Bank.

Technical & Functional Specifications - Compliance Parameters for Technical Evaluation

Sr. No.	**Specifications**	**Compliance with clear /explicit Supporting Documents** (Yes/No)	**Available as part of OEM solution** (Yes / No)	**To be made available as Customization or Third Party** (Yes / No)	**Feature availability (on Cloud/On-premises /Both)**
1.	Functioning of Software / Hardware / Network.	Attach supporting Documents			
2.	Licensing details of Software Solution / Service/ Product	Attach supporting Document			

TECHNICAL SPECIFICATIONS

(A) General Features:

Sr. No.	Specifications	Compliance with clear /explicit Supporting Documents (Yes/No)	Available as part of OEM solution (Yes / No)	To be made available as Customization or Third Party (Yes / No)	Feature availability (on Cloud/On-premises /Both)
1	The proposed Solution should be deployed in **Hybrid model** (Partly on Bank's premises and partly on OEM's Cloud) with the sensitive/critical data not leaving SBI's premises.				
2	The data at rest and data in transit should be encrypted as per best practices and also in line with Bank's IS Policy guidelines.				
3	Bank Data should never leave geographical boundaries of India either at rest or in transit.				
4	The proposed solution should be compliant to regulatory requirements of RBI, CERT-IN, Bank's ISD, SOC and other regulatory bodies in India offshore Regulatory bodies wherein SBI branches/admin/ offices are present in foreign locations.				
5	Solution should support high availability Active-Active or Active-Passive configuration for DC and DR setup. UAT setup also required at any one location i.e., DC or DR.				

6	Solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non-Windows Operating Systems including CDK, QMS and other customer touchpoint endpoints. Solution should protect all upcoming /upgraded OS in the Bank's IT ecosystem during the contract period. Solution should also protect other Roaming Clients external to Bank Network i.e., Mobile, iPad, Laptop running on Android/iOS and other firmware/ OS/s.				
7	OEM should have DR arrangement for release of updates including signatures and security updates.				
8	OEM and Bidder should have alternate infrastructure support arrangements available in India in case primary facilities are not available.				
9	The connectivity between the Bank's on-premises ESS infrastructure and OEM cloud or their cloud service provider should be through dedicated line i.e. (MPLS link) from two different telecom service provider via shortest route.				

B. Endpoint Protection Platform (EPP) and Early Detection And Response (EDR) Technical Features:

Bank's requirement is to protect each and every endpoint/Server in its environment from malware and IT-Threats. The proposed solution must be capable to use central data repository of the Bank's endpoints/Servers as well as Global central data repository of the OEM to observe and analyze endpoint /Servers' vulnerabilities and IT-Threats. ESS Solution should work toward stronger protection of the endpoints/Servers and appropriate remediation responses to the proactive IT-Threats. It must be an integrated endpoint

security solution that combines real-time continuous monitoring and collection of endpoint/Servers data with rules-based/behavior based/ heuristic based automated response with analytical capabilities. The solution should be capable to respond to advanced persistent threats, and any attack that manages to bypass preventative defenses on an endpoint/Server device. The feature of the desired ESS/EDR solution are as under:

1. EDR should not just have Signature based or files-based detection but should also have AI/ML and behavioral based detection.
2. EDR solution must have detection at rest capability.
3. Solution should be capable to incorporating threat intelligence database and is comparing all the endpoint activities with the IOCs from the database to detect many malicious activities within the environment.
4. The EDR sensor should provide remote shell to the system to get access and mitigate a malicious activity, it includes network isolation, and remote access.
5. EDR solution should have the capability of writing custom alerts for endpoints.
6. Solution should be capable to search the incident in data repository locally or globally on OEM cloud for investigate and remediation.
7. Solution should have the intelligence to generate alert during suspicious activity detection, validation and appropriate response.
8. Solution should have the intelligence for Threat hunting or data exploration.
9. Solution should have the intelligence to generate alert and Stopping malicious activity
10. Solution should have event correlation capabilities i.e. Anomalies whether volumetric or heuristic should be identifiable by the solution. As the solution would have capability to correlate data from accessed emails, files, URL, USB.
11. Solution should be capable for policies creation to control USB/devices usage based controls.
12. Solution should be capable to create an inventory of installed programs/software and should be available for risk assessment and quantification.
11. Solution should have the intelligence for User access details, local accounts and alert in case of suspicious behavior.
12. Solution should be capable of providing the visibility over chronological events that happened over endpoint which includes system as well as user activities.
13. Solution should use Artificial Intelligence/Machine Learning methodology for performing operations.
14. Integration with multiple tools.
15. EDR solution will be able to block/quarantine/isolate the system from network through ESS Central management server deployed in Bank irrespective of system connected through SB connect network or it is roaming endpoint.
16. Alerts, reporting, and a unified overview of IT environment.
17. Advanced response capabilities and automation.

Sr.No.	Specifications	Compliance with clear /explicit Supporting Documents (Yes/No)	Available as part of OEM solution (Yes / No)	To be made available as Customization or Third Party (Yes / No)	Feature availability (on Cloud/On-premises /Both)
1	The Endpoint Security Solution should be using a blend of AI/ML based advanced threat protection & detection techniques to eliminate threats entering in to SBI network services to be delivered via an architecture that uses endpoint resources more effectively, preserve and optimize CPU, network utilization to their lowest value.				
2	The solution must provide all listed features of proposed Endpoint security solution in a single lightweight agent. Solution must have a light footprint and agent based / agentless solution must have minimal /no impact on performance of endpoints.				
3	Solution should be able to defend endpoints on or off the corporate network against ransomware, malware, Trojans, worms, spyware, ransomware, and adapts to protect against known / unknown variants and advanced threats like crypto malware, file less malware and macro-based malware in				

	order to detect and respond to the ever-growing variety of advanced malware threats, including file and file less attacks and ransomware.				
4	The Solution must have Early Detection and Response capabilities with insightful investigative capabilities. Solution to have centralized visibility across the network by using an advanced EDR, strong SIEM integration, with open API integration features and threat intelligence sharing capabilities.				
5	Solution must have multiple techniques to address known, unknown, patched, unpatched threats with pattern / signature based, behavior monitoring, virtual patching. The solution should be able to identify vulnerabilities with highly accurate machine learning - pre-execution and runtime, application control & EDR features. The Solution should have both IOC & IOA based approach with the detection module mapped to MITRE ATT&CK framework for easy understanding of attack stages and lifecycle to the security analysts.				
6	Agents on endpoints must be updated via a centralized server and conserve WAN bandwidth with lowest utilization.				

7	The proposed solution should have option to configure policies based on the location of the endpoint, Desktop-wise and Server-wise. It should also have capability to create department wise or application-wise policy groups for servers and endpoints.				
8	Solution should provide agent self-protection to be configured via GUI or CLI.				
9	The solution must be FIPS 140-2 compliant, using encryption algorithms AES 256 bit or above. The feature should comply to best practices and Bank's IS Policy.				
10	Solution should have feature to configure client communication interval which defines how often endpoints report their encryption status and policy updates to central management console.				
11	The solution should support Multi-threaded scanning.				
12	The solution should have proactive and heuristic scanning and protection against known and unknown viruses and threats.				
13	The solution must have flexible server deployment options to match various types of environments.				
14	The Solution should have Automated Malware Analysis				

	capabilities and real-time threat detection.				
15	The solution should support detection of suspicious networks and Botnet that are carried by Any protocol.				
16	The solution should have Infection detection capabilities with/ without sandboxing features. The solution should support AI/ML based malware and threat detection.				
17	The solution should support client lock down feature for preventing desktop users from changing real-time settings.				
18	The solution should be able to detect and prevent hidden exploit processes that are more complex than a simple signature or pattern and evade traditional AV.				
19	The solution should have strong anti-evasion capabilities. It should also accurately identify evasion capabilities of malware such as evasion by detecting sandbox environment, sandbox artifacts, artificial environment, timing differences, evasion by using time, event or environment-based triggers, system events, user interaction, blinding the sandbox and ecosystem.				
20	The Solution should be able to perform the following correlations based on analysis rules mapped to various threat categories and provide				

	criticality information. The various threat categories to be covered include • Vulnerability based. • Statistical based. • Historical based. • Heuristics based. • Behavior based on source entity, applications. • Information Leak. • Unauthorized Access. • Denial of Service. • Service Unavailable. • Phishing attack • Pattern based rules • Profiling • Whitelist/ Blacklist/ Reference List • Applicable to Virtual environment endpoints. (Threats related to virtual infrastructure like hyper jacking, guest VM escape)				
21	Solution must support creation of rules to exclude specific addressed / IP ranges, Country/Countries and provide capability for Blacklisting malicious IPs/ countries and domains.				
22	Solution must identify and block privilege escalation attacks Specially root level attacks like rootkit, bootkit or any other such malwares and provide Process monitoring mechanism.				
23	Solution must identify and block/alert on lateral movement (SMB relay, pass the hash) and provide Network traffic				

	monitoring originating from endpoints.				
24	Solution should be able to pinpoint the origin of attack.				
25	Solution must support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as • Capability of running a coordinated command (such as CMD interface). • Running script or a file from a network location or mapping a drive. • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network and should support for virtualized infrastructure as well. • Deletion of a file (including active run files). • Put file into quarantine (including active run files). • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Blocking telecommunications based on destination (domain address or IP address). • Disconnection of network cards.				

	• Capability of editing a HOST file. • Renewed operation of an end station and/or a server. • Include Damage Cleanup Service functionality which addresses changes to the Windows registry and other similar malicious alterations.				
26	Solution must provide log collection and retention such as Collect authentication, activity logs and retain them for the period of time that is required by various regulations.				
27	Solution must support rapid and seamless installation across all endpoints and servers for approx. 4,00,000 (Four Lakh) endpoints in a single installation/ environment.				
28	Solution must support automated distribution on endpoints/servers after the initial installation. Also, should automatically discover newly added machines and have the agent installed on them without need of manual configuration.				
29	Solution must co-exist with all commodity and proprietary software on the endpoints\servers and provide seamless operation of the protected endpoint/ server without bluescreens or process crashes.				
30	Solution must collect endpoint, file, process, user				

	activity and network traffic in a fully self-sustained manner such as Eliminate the need of manual configuration of rules or policies or reliance of additional devices.				
31	Solution must have the ability to enable/disable certain types of notifications				
32	Solution must provide a central collection and processing of alerts in real-time.				
33	Solution should be able to perform Threat Analysis of Endpoints for inspecting to uncover issues such as file less malware prevention and web browser base attacks prevention.				
34	Solution should provide proactive, immediate notifications of serious system health issue for the solution.				
35	Solution must be able to detect when system sleep functions are used by the malware to evade detection and accelerate the time to force the malware into execution				
36	Solution should have a stateful attack analysis to detect the entire infection lifecycle and trace stage by stage analysis of the advanced attacks from system exploitation to outbound malware communication leading to data exfiltration.				
37	Solution must assist in detecting the movement of human intruder to multiple				

	systems using different tools for any lateral movement.				
38	Solution must detect and handle the presence of malicious files that have been written to the systems but not executed.				
39	Solution should have capability to analyze obfuscated and encrypted malware.				
40	Solution should have built-in vulnerability assessment such as Discover missing security updates within systems and applications.				
41	Solution should provide Advanced Threat Intelligence platform, unlimited structured, unstructured threat intelligence gathering from combination of Commercial, Open source, user led, community based, and industry driven with proactive advisory solution capability from OEM for existing as well as new threats including Zero-day threats to enable Bank to enforce countermeasures to contain risk.				
42	Solution must ensure the following elements but not limited to the IOCs: i. Source information (IP, Domain, URL) ii. File formats (.exe, .doc, .pdf, .xml) iii. Geo Location iv. File hash values v. Vulnerability details.				

43	The threat intelligence interface should include complete threat visibility i.e., End-to-end details of threats such as attack surface vulnerabilities, malware, IOCs, IOAs, actors behind the attacks, tools, tactics, and procedures used, motivation.				
44	Solution must assess threat intelligence and proactively identify / visualize impact, exposure to Bank's environment, understand the existing controls, determine residual risk to Bank and provide the complete remedial solution.				
45	Solution must have the ability to specify a list of alert exclusion rules for the selected objects.				
46	Updates of Solution should be capable of being rolled back with minimum time duration incase required on Endpoint Security Solution infrastructure as well as on end points.				
47	All binaries from the OEM (Vendor or system) that are Downloaded and distributed must be signed and signature verified during runtime for enhanced security.				
48	Solution should have password protection to disable configuration changes / uninstall by unauthorized personnel/ malware				
49	Solution should be capable of scanning the system during				

	booting process and detect and remove boot sector virus or root kit.				
50	Solution must detect and prevent any buffer overflow.				
51	The solution should support vulnerability remediation irrespective of the exploit that is trying to use the buffer overflow vulnerability.				
52	Solution should provide Digital Identity Protection (protecting personal information from being leaked)				
53	Solution should provide protection against banner attacks (advertisements, pop-ups)				
54	Solution should provide protection from key loggers.				
55	Solution should have file caching to avoid repetitive scanning of files which are unchanged since the previous scan.				
56	Solution should allow to configure different policies for different set of processes.				
57	Solution must scan for hidden processes, and other behavior that suggests malicious code is attempting to hide itself and effectively remove the program without degrading system performance.				
58	Solution should not allow the user to uninstall or disable Endpoint Security Solution agent				
59	Solution should have the capability for sandbox				

	/without sandbox /AI-ML model-based malware detection. Solution should support Sandboxing components deployment in Bank premise only.				
60	The AI-ML model-based or sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks.				
61	Solution should provide file repudiation service that can restrict executable file download based on prevalence, source, and age.				
62	Solution must be able to restrict device access on endpoints by assigning rights to allow or deny the Read, Read/Write, and Write and execute, copy. The Devices that are able to be restricted must include the following: - USB Drives (Also have feature to disable auto run) and other type of device control. Configuration for Device Access Control must be done centrally from the management console.				
63	Solution should provide policy inheritance exception capabilities.				
64	Solution should have the ability to lock down a computer (prevent all communication) except with management server.				

65	Solution should integrate with Hypervisors like VMware ESXi with/without the need to install agents on the guest VMs and all other Hypervisors available in market and use by corporates/industry.				
66	Solution should protect against Distributed DoS attacks.				
67	Solution should provide security from hyper jacking and guest VM escape in case of Virtualized environment.				
68	Solution should support Endpoint Security Solution infrastructure i.e., management and administration console of Endpoint Security Solution on Virtual environment of Bank or alternatively vendor should provide scalable hardware /software / infrastructure supplied for implementation of overall ESS Solution within the overall cost for the entire contract period of 5 years.				
69	Memory footprint – cache and signature database size should be limited and minimum, solution should have ability to deal with agent bloat problem, should have capability to take optimal use of network resources (for updates and intra VM communication for intelligence sharing (if any).				
70	Memory monitoring - While the process is running in the				

	memory, its behavior is observed to decide if it could be a virus. Solution should also support detection and prevention from phishing and rogue apps.				
71	All endpoint agents like (desktops, windows servers, Linux servers, virtual machines. iPad, Mobile, and roaming/remote systems) deployed as the Bank's assets should be monitored / manageable through a single orchestrator/management console.				
72	Solution should support Single integrated workflow to analyze and respond to threats within Endpoint Security.				
73	Solution should support Enterprise Security Search to rapidly find and illuminate suspicious activity and threats.				
74	Solution should support Data Acquisition to conduct detailed in-depth endpoint inspection and analysis over a specific time frame.				
75	Solution should support End-to-end visibility that allows security teams to rapidly search for, identify and discern the level of threats				
76	Solution should have capabilities for Detection and response to quickly detect, investigate, and contain endpoints to expedite response.				
77	Solution should Support Easy-to-understand interface for fast interpretation and response to any suspicious endpoint activity.				

78	Solution should have the capabilities for resolution of issue by • Deleting malicious files and associated artifacts on all impacted endpoints. • Blacklisting and whitelisting files at the endpoint				
79	Solution should support Investigation and ensure threat containment by complete and continuous incident logging of endpoint activity, view specific endpoint processes				
80	Solution should support to Contain potentially compromised endpoints during investigation with endpoint quarantined.				
81	Solution support Integration and Automation for unify investigator views, orchestrate data and workflows by • Easily integrate incident data and actions into existing Bank SOC infrastructure. • Replicate the best practices and analysis of skilled investigators with automated incident rules list. • Gain in-depth visibility into endpoint activity with automated artifact collection				
82	Solution should support Attack Analytics and Endpoint Advanced Attack Detections.				
83	Solution should support complete and Rapid endpoint Repair and also support detection and prevention from phishing and rogue apps.				
84	Solution should automate the complex, multi-step				

	investigation workflows of security analysts from Historic data.				
85	Solution should support to build AI / ML based intelligent model/s and databases to quickly expose suspicious behaviors, unknown threats, lateral movement, and policy violations				
86	Solution should support creation of AI / ML based intelligent model/s and databases to automate best practices and document specific threat hunting scenarios.				
87	Solution should support remote shell to the machine to mitigate a malicious activity this includes network. isolation and remote access.				
88	Solution must have Noise cancellation techniques like reputation services and whitelist checking at each layer to reduce false positives. The solution should support inline blocking mode as well as monitoring mode and should have a low or Zero false positive rate. Solution should have mentioned Scanning capabilities – in-memory malwares, registry changes, and system component changes, behavioural analysis, HIPS, lateral movement of malwares should be detected.				
89	Should have a manual outbreak prevention feature that allows administrators to configure port blocking, block shared folder, and deny				

	writes to files and folders manually.				
90	Solution should support the scanning of all the endpoints immediately after deployment of any new model/engine and signature on all the endpoints for presence of the malwares hitherto. Solution must also support various scanning options to clean dormant malwares - Real time scan, Scheduled Scan and on Demand Scan				
91	The solution should support to block / quarantine / clean the viruses/threats for the hashes/signatures given by various advisories (i.e., CERT-In, RBI and Bank) from time to time through OEM's global engine. OEM's/SI should provide and deploy dedicated engine on endpoints to take corrective and preventive action for hashes/signatures provided through advisories within SLA timelines.				
92	The solution should have capabilities to detect/prevent/block/quarantine/clean all kind of IT threats by EDR or conventional method such as • Anti-malware • Rootkits/grayware scanning for file system to prevent or stop spyware execution. • Should have capabilities to restore spyware/grayware if the				

	spyware/grayware is deemed safe. • Behavior Monitoring • Device Control • Real Time Scan • Suspicious connection services • Web Reputation Services • Application Change Control (ACC) • File Integrity Monitoring (FIMS) • File-less malware protection • Macro-based malware protection • Memory-based malware protection • Protection from Boot and rootkit malware. • Phishing and rouge apps protection • Zero-day attack protection. • Protection against vulnerability in OS in absence of patches and hotfixes from OEMs • Protection against indicator of attack. • AI/ML based pattern and behavior analysis. • Anti-Ransomware				
93	To address the threats and nuisances posed by Trojans Worm, Hoax, Virus, the solution should be able to do the following: a. Terminating all known virus processes and threads in memory. b. Repairing the registry.				

	c. Deleting any drop files created by viruses d. Removing any Microsoft Windows services created by viruses. e. Restoring all files damaged by viruses f. Includes Clean-up for Spyware, Adware. g. Solution will be able to scan only those file types which are potential virus carriers (based on true file type).				
94	Solution must support a distributed framework for signatures and policy to have provision and capability to assign a client the privilege to act as an update agent for rest of the agents in the network.				
95	Solution must have the ability to specify a schedule for downloading updates, Including the ability to disable automatic update. Also, taking care of update storms which may choke the bandwidth. Solution should have automated recommendation of integrity rules to be applied as per applicable server OS and can be scheduled for assignment / assignment when not required. Solution should provide a report on list of machines where scheduled scans not completed or outdated systems for a defined time period. It should also provide reports for top 10 virus infected systems Bank wise/				

	group-wise/ IP Address infected.				
96	Solution should be able to perform different scan Actions based on the virus type (Trojan/ Worm, Hoax, Virus, other and shall be able to scan only those file types which are potential virus carriers (based on true file type). Solution must support the means to execute forensic investigation and provide investigation data such as • Running process\file. • Machine level. • Memory activities. • Obtain memory dump. • Programs like mpress, compress a file in such a way that their hash value/Signature changes. • Deep file inspection should be able to prevent it.				
97	Solution should provide social Engineering attack visibility for e.g.: attackers exploiting vulnerability found in docs such as pdf. Provide protection from real time browser-based attacks.				
98	Solution should be able to identify suspicious embedded object in document file like OLE & Macro extraction, Shell code & exploit matching.				
99	Machine learning module should be able to extract multiple features from file for e.g.: who, when, where info, import table, header, opcode, packer existence. and compare it with				

	cloud/on-prim machine learning model and predict the maliciousness of the file. SBI is expecting to have strong machine learning module to address unknown threats.				
100	Solution must show the assigned confidence/score in terms of Percentage in the ML based detection logs to show the predictiveness of the Threat.				
101	Solution should have capability to Detect and Expose threats by using • Machine Learning and Behavioral Analytics to expose suspicious activity, detect and prioritize incidents. • Automatically identify and create incidents for suspicious scripts and memory exploits. Expose memory-based attacks with analysis of process memory				
102	Solution must have behavior monitoring module to constantly monitor endpoints for unusual modifications to the operating systems and installed software's.				
103	Behavior monitoring must have program inspection to detect, and block compromised executable files. Behavior monitoring should monitor for newly encountered program downloaded from various channels like web/email/removable media.				
104	Solution must include threat hunting and provide Search				

	for malicious presence by known IOC (Indicators of Compromise), IOA (Indicators of Attack) like Shell modification, host file modification, library injection, new service process modifications, duplicated system files, malicious PowerShell credential access. Solution must have capability to block Indicators of Compromise (IOC) and Indicator of Attack (IOA) internally as well externally received IOC. Solution should support Fully integrated malware protection with antivirus (AV) defenses, machine learning, behavior analysis, indicators of compromise (IOCs) / (IOA's) and endpoint visibility.				
105	Behavior monitoring must have Anti-exploit capabilities 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. Application exploits prevention to stop "backdoor" entries and are common in third-party applications and outdated operating systems. Protect against exploits of unpatched				

	OS and third-party application vulnerabilities. Solution should be capable to prevent execution of all unauthorized software, scripts, and dynamic-link libraries (DLLs) and further defend against memory exploits.				
106	Anti-exploit capability must support various exploit prevention techniques but not limited to Force ASLR, Null page, Heap spray.				
107	Behavior monitoring must have multiple action parameters such as assess, allow, block, deny, terminate.				
108	Solution must support Browser Exploit Prevention - scan browsers for exploit/script/scan webpage and Block.				
109	Solution should be able to handle and have capacities for protection and recovery from threats like ransomware, browser exploit, web reputation, Advanced persistent threats or any new or anticipated threats. Ransomware protection must not be limited to specific ransomware behavior /variants.				
110	Solution should support rollback / restoration of the endpoints to its last good state in case the endpoints are infected by ransomware or by any other IT Threat method. Should support				

	logging reporting and correlation of suspicious events.				
111	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.				
112	Solution must be able to block all communication to Command & control center-bad IP/domain.				
113	Solution must support adding whitelisting and Blacklisting of URL's/Domain using wildcards.				
114	Solution must provide by default security levels i.e., High, Med & low so that it eases the operational efforts and Solution must have an option of assessment mode ONLY so that URLs are not blocked but logged.				
115	Solution must be able to detect/prevention communications to Global C&C's and Allow administrators to create user defined list also.				
116	Solution must support malware network fingerprinting mechanism to detect unique malware family signatures within network packets and just not rely on IP addresses/domains.				
117	Solution must have damage clean-up services after				

	detecting Command & Control communication.				
118	ESS solution should be capable to protect the endpoints from OS related vulnerabilities by automated virtual patching/scripting/tool base protection of the endpoints in absence of patch/fix release by OS vendor.				
119	Solution should have deep packet scrutiny, Integrity monitoring, Log scrutiny and correlation capability to identify content that may harm the application layer, Filters forbidden network traffic and ensures allowed traffic through stateful investigation.				
120	HIPS engine should have multiple configuration options i.e., Inline or tap mode-Detect only.				
121	Solution should have multiple types of rules i.e., Vulnerability, exploit and general rules.				
122	Solution should have capability to have IOC, IOA and MITRE ATT&CK mapping for detections like: • Reverse Shell communication (ATT&CK T1071). • Remote command execution via WinRM (ATT&CK T1028), • Domain level -Credential dumping over DCERPC (ATT&CK T1033). • WhatsApp Communication attempt (ATT&CK T1102).				

	• Remote file copy over FTP (ATT&CKT1105). • Remote Service creation (ATT&CKT1050). • Block Admin Share (ATT&CK • T1077, T1105				
123	Solution must have default modes of either performance or security priority.				
124	Solution should deliver the most-timely vulnerability protection in the industry across a variety of endpoints, including end-of-support (EOS) operating systems.				
125	Solution must provide context-aware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack. EDR must record User and Kernel level operations - activities related to File, Process, User, Registry, DNS, Memory, IP, Port.				
126	Solution must support Indicator of Compromise (IOC) - Sweeping on the basis of: • User File name, File hash, Fqdn / IP / hostname, Registry - key, value name, value data cli command. Solution must have capability to block Indicators of Compromise (IOC) and Indicator of Attack (IOA) internally as well externally				

	received IOC. Solution must have capability to create threat feed for internally developed indicators of compromise (IOC).				
127	Solution must support Device control - Whitelisting/Blacking listing of devices.				
128	Solution must support Allow/Block Actions for the supported devices.				
129	Solution must support scanning of Network Devices, USB, Mobile Storage, Non-Storage devices, Bluetooth adapter, Com/LPT, Imaging, Prt Scrn key, and Wireless Nic for identification of threats on endpoints (Desktops). If required Bank should implement these features for servers also.				
130	Solution must support various permission -Full Access, read only, Execute, Modify				
131	Solution should have minimum following format supported for threat Intel ingestion, processing and sharing. STIX / TAXII, Yara rules, Open IOC, JSON, XML. Solution should also provide User Defined Repository received from Other deployed products.				
132	Solution should support cyber data analytics, forensic analysis, investigation automation, Threat Investigation - Historic, Live, and Scheduled, SBI may use any				

	of the option depending on the scenario.				
133	Solution must support Attack Discovery - Indicator of Attacks monitoring endpoint activity for Attacker's intent and Tactics, Techniques and Procedures being used.				
134	Solution must support Indicator of Attacks (IOA) with MITRE ATT&CK Framework - few examples: • Tactics: Credential Access Account Creation Privilege escalation Defense evasion Execution Lateral Movement Exfiltration Persistence				
135	Solution must support live investigation to look for process running in memory, file existence on Disk, registry value/key on the endpoints. The solution must identify malicious behavior of executed files\running processes\registry modifications\ memory access and terminate them at runtime, and raise an alert (exploits, file less, Macros, PowerShell, WMI) and provide Memory access monitoring, Process behavioral analysis (heuristics) High similarity (i.e., fuzzy hashing). The Solution must identify and fix/protect from these kinds of vulnerabilities.				
136	Solution must have an option of doing impact analysis - if specific Threat seen on				

	endpoint can be swept across enterprise. Solution must support the means to execute forensic investigation and provide investigation data such as •Running process\file. • Machine level. • Memory activities. • Obtain memory dump. • Programs like mpress, compress a file in such a way that their hash value/Signature changes. • Deep file inspection should be able to prevent it.				
137	Solution must support giving details like command / registry /rating of the object and isolate the Endpoints without generating Root cause/Attack chain. Solution should provide Pre and post compromise attack visibility (Root Cause Analysis) as well as provide Fast incident triage, investigation, and response.				
138	Solution must have Root cause analysis for simple or full Root cause/Attack chain, SBI expects Root Cause chain to be interactive so that immediate actions like adding to suspicious objects list, terminating, investigating should be the option available in the chain. RCA should indicate objects in different colors for easy analysis for e.g.: malicious, suspicious, known good.				
139	Solution must support below response options:				

	Endpoint isolation - communicates with management only Customize rules during isolation Endpoint Restoration Terminate Process Block -IP address Block Hash Block Domain/URL Block/Quarantine - File Outbreak prevention - deny access to file/folder, ports, block write access, and deny access to executables. Suspicious Repository -to be shared with existing deployed products. Solution should discover and report the hostname/IP address of the infected source that send the malicious code in to the network, block further communication from the infected source for configurable time period.				
140	Solution must support API for collecting logs, Investigation, Isolation/restore, Running Root cause analysis/Sweeping.				
141	Solution should have capability of integration with • Active Directory Services. • Privilege Integrity Management Systems (PIMS). • Network Access Control (NAC) and NTP (Network Time Protocol).				

	• IT Asset management ITAM. • Security incident management SIEM, DAM and Bank SOC solution. • Bank's Proxy solution. • Firewalls, IDS, IPS for Threat Intelligence. Solution should also be able to Integrate with other security products locally or on OEM hybrid cloud /network and also to deliver network sandbox rapid response updates to endpoints when a new threat is detected, enabling faster time-to-protection, and reducing the spread of malware.				
142	Centralized security management console should ensure consistent security management and complete visibility and reporting across multiple layers of interconnected security.				
143	Central Management server of the Endpoint Security Solution should be able to monitor the status of AV service on the endpoints. In case the service is down, there should be a mechanism to automatically restart the service from the central manager.				
144	Console should have an option of creating custom dashboard and report as per SBI's requirement. Tabs and widgets support, Threat Events History (Detection over time), Threat				

	Classifications/Types				
145	Console should have an option of creating users with different user roles for managing the solution.				
146	Console should have an option of doing impact analysis of threat seen on endpoint and check other endpoints for the same. The centralized management console should deliver security threat information including current threats and future threats also.				
147	Management console should be able to integrate with Active Directory, two factor authentications.				
148	Solution must extend visibility and control across on-premises and/or hybrid deployment models. Centralized management combines with user-based visibility to improve protection, reduce complexity, and eliminate redundant and repetitive tasks in security administrator.				
149	Management console should have an option of various alerting methods such as Email/SIEM integration.				
150	Management console should support API integration.				
151	Solution must support Reporting option with One time/Scheduled/Custom in CSV / PDF / RTF, Excel, Word, PowerPoint, or any other format desired by the Bank.				

152	Solution must support Automatic sharing of threat intelligence across security layers enabling protection from emerging threats across the whole organization.				
153	Solution should have a provision of creating user defined repository where file/URLs/hashes can be added and shared among other security products. Solution should have Threat Intelligence, forensic Capabilities. It should also have data collection feature to build a repository for analytics				
154	Solution must have Detection and Response option to have Native integration with products for events correlation across Endpoints, Network, Email, and hybrid Cloud to reduce overall MTTD and MTTR for SBI.				
155	Solution must have central repository of threat intelligence - powered with 01 trillion+ threat queries and more than 10 Billion threats per day, sensors, and multiple sources of threat information and same should be available as update for SBI.				
156	The solution should be able to protect against Advanced Malware, zero-day, web exploits and targeted threats without relying on signature database. The solution should provide facility of virtual patching /				

	protection to fix zero-day attacks on the basis of OS vulnerabilities for which fix are not available or released by OEMs. Solution must scan for Rootkit, zero-day attacks and effectively remove the Rootkit without degrading system performance.				
157	The proposed server security solution must support multiple platforms of server operating systems i.e., Windows and non-windows i.e., MacOS, Unix, Linux-RedHat, CentOS, Oracle, Debian, SUSE, Ubuntu, Solaris, AIX, Amazon Linux, Cloud Linux and any other existing or new/upgraded OS flavors during the contract period. Server security Solution must support the following indicative list of server operating system but not limited to: • Microsoft Windows Server 2008 &2008 R2, 2012 & 2012 R2, 2016,2019. • RHEL 6,7,8. • CentOS 6,7,8. • Ubuntu 16,18,20 • Debian 8,9,10 • Solaris 10.0,11.0,11.1,11.2,11.3,11.4 • Oracle Linux 6,7,8 • AIX 6.1,7.1,7.2 • SUSE Linux 12,15 • HP UX all versions Any other legacy, existing and new OS in Bank during contract period. Solution should support protection of physical as well as virtual				

	instance of all servers OS flavors				
158	All prevention capabilities as best practice in industries for servers i.e., Antimalware, HIPS, Firewall, Application control, FIMS, Log correlation, Command & Control or suspicious network prevention should be delivered through the single agent managed through the centralized management console.				
159	Solution should provision inclusion of packet data on event trigger for forensic purposes. The solution should support agent-based or agent-less for server security that: • Support Deep Packet Inspection (IPS/IDS) • Support Anti Malware • Integrate with Hypervisors like VMware ESXi or NSX firewall with or without the need to install agents on the VMs. • Should support all flavors of Virtual Servers like Hyper-V, VMware ESX, ESXi, NSX firewall and future variants and containers.				
160	Deep packet Inspection should protect operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injections and cross-site scripting.				
161	Solution should provide ability to automate/script				

	base/tool base rule recommendations against existing vulnerabilities, exploits, suspicious network traffic and dynamically tuning IDS/IPS sensor (E.g., Selecting rules, Configuring policies, updating policies)				
162	Solution should support creation of customized DPI rules if required.				
163	Solution should provide recommendation for automatic/script base/tool base removal of redundant rules if a vulnerability or software is patched/upgraded - E.g. If a patch is deployed or software is uninstalled corresponding redundant rules to be automatically removed.				
164	The solution should allow imposing HTTP Header length restrictions.				
165	The solution shall have the capability to inspect and block attacks that happen over SSL.				
166	The Solution should track the infection or threat history for a device, with the ability to access all forensic evidence from past infections. Solution should have Threat Intelligence, forensic Capabilities. It should also have data collection feature to build a repository for analytics				
167	Solution should be capable of blocking and detecting of IPv6 attacks. The solution should scan all types of				

	traffics including HTTP, FTP, HTTPS, SMTP for viruses, malwares, spywares.				
168	Solution should offer protection for virtual, physical, cloud and Docker container environments.				
169	Deep Packet Inspection should have Exploit rules which are used to protect against specific attack variants providing customers with the benefit of not only blocking the attack but letting security personnel know exactly which variant the attacker used (useful for measuring time to exploit of new vulnerabilities).				
170	Deep Packet Inspection should have pre-built rules to provide broad protection and low-level insight, for servers. For operating systems and applications, the rules limit variations of traffic, limiting the ability of attackers to exploit possible attack vectors. Generic rules are also used to protect web applications (commercial and custom) from attack by shielding web application vulnerabilities such as SQL Injection and Cross-Site Scripting				
171	Solution should support automatic and manual tagging of events.				
172	Solution should support CVE cross referencing when applicable for vulnerabilities.				
173	The solution shall protect against fragmented attacks				

174	The solution should allow to block based on thresholds				
175	Deep packet inspection should have signatures to control based on application traffic. These rules provide increased visibility into & control over the applications that are accessing the network. These rules will be used to identify malicious software accessing the network.				
176	Solution should have Security Profiles which allows DPI rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required. Rules should be auto- Provisioned based on Server Posture. De-provisioning of rules should also be automatic if the vulnerability no longer exists.				
177	Solution should support excluding certain file, directories, file extensions from scanning (real time/schedule).				
178	Solution should use a combination of hybrid cloud-based threat intelligence combined with traditional endpoint security technologies.				
179	Solution should support True File Type Detection, File extension checking. Solution must scan nested compressed files (a minimum of 5 level)				

	for malwares, viruses, spywares and should support various algorithms such as ZIP, LZH/LHA, ARJ, MIME/UU, CAB, Arc Manager, Ghost Image, BinHex, RAR, TAR, UUE, Executable files, GNU, HTTP, Microsoft compressed, LESS Containers, Rich text format, MS-TNEF, 7ZIP, GZIP. This should also include malware mutation like mpress compression which changes hash values				
180	Solution should support heuristic technology for blocking files containing real-time compressed executable code.				
181	The proposed solution should be able to detect and prevent the advanced threats which come through endpoint client-side executable files, PDF files, Flash files, RTF files and and/or other objects using Machine learning. The solution should be able to identify malware present in network file share drives and web objects (For E.g.: JPEG, doc, docx, exe, gif, hip, htm, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx. and any other new formats having vulnerabilities carry potential malware) and able to quarantine /block/clean.				
182	Solution OEM should have Threat Intelligence, forensic Capabilities. It should also				

	have its data collection network and features to build a strong repository for ingestion into analytical based models for threat detection. Solution should support cyber data analytics, forensic analysis, and investigation automation.				
183	Solution deployment should cause limited interruption to the current network environment.				
184	Solution should have a Log scrutiny services which provides the ability to collect and analyze operating system, databases and applications logs for security events. Solution should be capable of providing services such as • Deep Packet Inspection (HIPS/HIDS). • Anti-Malware/ransomware. • Integrity monitoring. • Log scrutiny.				
185	Solution should provide predefined out of the box rules for log collection from standard applications like OS, Database, web Servers and app server and allow creation of custom log scrutiny rules as well.				
186	Solution must have an option of automatic recommendation of rules for log analysis as per the Server OS and can be scheduled for automatic/script/tool base assignment/un-assignment of rules when not required.				

187	Solution should have ability to forward events to an SIEM system or centralized logging server for eventual correlation, reporting and archiving.				
188	Log scrutiny rules should allow setting of severity levels to reduce unwanted event triggering.				
189	Customized rule creation should support pattern matching like Regular Expressions or simpler String Patterns. Automatic rule should be triggered on a match.				
190	Solution should have ability to set dependency on another rule causing the first rule to only log an event, even if the dependent rule specified also triggers.				
191	Solution must support decoders for parsing the log files being monitored.				
192	Solution should allow administrators to control what has changed on the server compared to initial state.				
193	Once the policies are deployed, the agents should continue to enforce the policies whether the management server is available or not.				
194	Agent installation methods should support manual local installation, packaging with third party software distribution systems and distribution through Active Directory.				

195	Solution should be able to update definitions & scan engine on the fly, without a need for reboot or stopping of services on system.				
196	Any policy updates pushed to the agent should not require stopping the agent, or to restart the system and Solution should provide ability to hide agent icon from getting displayed in system tray.				
197	Product should have the capability of supporting new windows/ new Linux kernels, any other legacy, existing and new OS in Bank during contract period as & when they are released. Solution should also support protection of physical servers as well as virtual instance of servers.				
198	The solution shall allow to do all configurations from the central management console like enabling/disabling agents, selecting and applying new policies, creating custom policies, reports.				
199	The solution should give the flexibility of deploying features either as agent based or agentless for different modules depending on organization's data center environment.				
200	The solution shall have the capability to disable the agents temporarily from the Central Management console & such action should be logged.				

201	The solution should have comprehensive Role Based Access Control features including controlling who has access to what areas of the solution and who can do what within the application.				
202	Solution should provide greater insight into threat outbreaks with user-based visibility, policy management, and log aggregation with ability to access all forensic evidence from past infections. It should enable reporting across multiple layers of security solutions.				
203	The solution shall allow grouping security configurations together in a policy and also allow to apply these configurations to other similar systems.				
204	The solution should support forwarding of alerts through E-Mail.				
205	The solution shall allow creation of custom lists, such as IP Lists, MAC lists that can be used in the policies that are created.				
206	Administrators should be able to selectively rollback rules applied to agents.				
207	Solution should have an override feature which would remove all the applied policies and bring the client back to default policies.				
208	The solution shall allow updates to happen over internet, over Leased Line with OEM Data Centre, or shall allow updates to be				

	manually imported in the central management system and then distributed to the managed agents. Additionally, solution must also have an option of defining machine to be updater relay only. Solution must provide automated and centralized download and deployment of all latest virus signature/patterns if any updates on a daily basis to servers across different OS platforms. The proposed solution should support both push and pull mechanism for virus signature updates. The default should be pull mechanism.				
209	Solution should have API level integration with public cloud service providers like AWS, Azure from the management console.				
210	The solution should be able to push policy from Bank's Centralized Management ESS solution on systems that are outside the Bank's network (for roaming clients)				
211	In case of mobile devices, the solutions must check for if the devices are rooted & permission assigned to the app.				
212	Data if needed to be pushed to OEM's cloud should be defined and known to Bank with all details and type of data. The Bank should be able to restrict and parametrize data attributes to be sent to cloud component as a part of telemetry data, if desired so.				

213	The roaming clients should connect to the on-premises components for sending any telemetry data / AV scan results. Though they can connect to cloud component for the threat database update / AV database update / version upgrade (specific details to be pushes by security policy from on-premises solution)				
214	The solution should automatically engage in an aggressive scan mode if it detects large number of malware or high-risk threats on clients.				
215	The solution should detect malware that evades detection by using polymorphic custom packers by unpacking in a lightweight virtual environment with no performance over-head.				
216	Solution should act as an integrated security platform and should provide visibility into network traffic and user activity, along with endpoint-specific activity and validate the suspicious behavior to generate true-positive Alerts.				
217	End point security solution (ESS), which should comprise the integrated agent for all Endpoint Protection Platform (EPP), Application Change Control (ACC), File Integrity Monitoring (FIM) and Endpoint Detection and Response (EDR) , if multi-OEM vendor collaboration is required . it should be the responsibility of all OEM to				

	manage internal integration for required features of agent supplied to Bank				
218	Solution should be able to prevent and block runnable/executable malicious viruses/worms/malware/logic bombs or any other security threat.				
219	Solution should be able to prevent and Block the files with embedded malicious payloads. i.e. Solution should able to block malicious codes/snippets/scripts/macros embedded inside normal PDF, MS Office Files (xlsx, docx, pptx), Archive files(zip,rar,7zip), Images(JPG, GIF, PNG) and various other Container File Formats.				
220	Solution should be able to prevent and block the files having exploit content of known/common vulnerabilities (NVD, CVE) of any common programming languages.				
221	Solution should support for defining and executing custom signatures using technology such as YARA rules to detect highly targeted malwares				

(C) APPLICATION CHANGE AND CONTROLS (ACC) FEATURES

Bank requires best security practices that blocks or restricts unauthorized applications from executing in ways that put Bank's systems/applications/data at risk. The control functions may vary based on the business purpose of the specific applications used in Bank, but the main objective is to help ensure the authenticity, privacy and security of the applications/systems and data used and transmitted by authorized applications. The proposed solution should have capability to integrate with Bank's APM (Application Portfolio Management Solution) or other existing solution with advanced API integrations,

AI/ML/behavior analytics model. The solution should enable application whitelisting through centralized management console for monitoring and enabling applications/services running across all endpoints/servers in the Bank.

Bank have grown increasingly dependent upon applications in day-to-day financial and other business operations. With web-based, cloud-based, and third-party applications at the core of today's financial transaction and business processes, Bank have challenge of monitoring and controlling data security threats while operating efficiently and productively. ESS solution should support Application Change and Control (ACC) module which include whitelisting and blacklisting capabilities to show which applications to be trusted and allowed to be executed in the Bank's IT environment. With Application Change Control, Bank can eliminate the risks posed by malicious, illegal, and unauthorized software and network access. The ACC Module should support AI & ML based methodology to identify the authorized applications / API's (standard as well as in-house) and keep track of changes in these applications. Bank's requirement is to implement all ACC features/functionality on endpoints and Bank will implement ACC's limited/critical feature/functionality on Servers also.

Sr.No.	**Specifications**	**Compliance with clear /explicit Supporting Documents** (Yes/No)	**Available as part of OEM solution** (Yes / No)	**To be made available as Customization or Third Party** (Yes / No)	**Feature availability (on Cloud/On-premises /Both)**
1	Application Change Control module should enhance Bank's 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				**On-premises**
2	It should Prevent potential damage from unwanted or unknown applications (Executables, DLLs, Windows App store apps,				**On-premises**

	device drivers, control panels, and other Portable Executable (PE) files).				
3	Solution should provide global and local Real-time threat intelligence based on good file reputation data correlated across a global network. solution must have an option of importing application list to the management console				**On-premises**
4	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.				**On-premises**
5	Solution must support importing inventory of hashes to define an Application change control criterion.				**On-premises**
6	Solution must contain broad coverage of pre categorized applications that can be easily selected from application catalogue (with regular updates).				**On-premises**
7	Solution must ensure that patches/updates associated with whitelisted applications can be installed, as well as allowing update programs to install new patches/updates, with trusted sources of change.				**On-premises**
8	Solution must support system lockdown to harden end-user systems by preventing new applications from being installed and executed apart				**On-premises**

	from the inventory found during policy installation.				
9	The solution should be able to conduct forensic analysis on historical data.				**On-premises**
10	Solution should be capable of locking and unlocking the server on the whitelist created by application change control.				**On-premises**
11	Reduce the risks and costs associated for malware associated with unauthorized application.				**On-premises**
12	Improve overall network stability by controlling applications available on systems.				**On-premises**
13	Identify all applications running within the endpoint environment.				**On-premises**
14	The solution should be capable of automatically accepting new software/application added which are already whitelisted through policy for connected and disconnected endpoints				**On-premises**
15	The Endpoint Administrator Users with physical or remote access to the machine should not be able to override protection.				**On-premises**
16	The solution should be able to define specific policies for specific sets of user/groups depending upon the requirements				**On-premises**
17	The solution should be capable to augment blacklisting and real-time reputation awareness. Prevent unauthorized applications from executing which may be malicious, untrusted, or unwanted as decided by the Bank.				**On-premises**

18	The solution should have a small overhead footprint which includes windows and non-windows endpoints / servers available in Bank IT ecosystems, mentioned elsewhere in this RFP.				**On-premises**
19	The solution should be capable to protect against memory-based attacks and application tampering. It should also cover cases where the name of the application/application's exe is changed by the user				**On-premises**
20	The solution should be capable to offer control over the applications, based on the information of the Applications (name, checksum)				**On-premises**
21	The solution should be capable to update the whitelisted applications locally and dynamically when trusted and authorized changes are implemented. The solution should be capable to maintain whitelisting records locally so that it works in offline mode as well.				**On-premises**
22	The solution should be capable of allowing only authorized applications to run and should block any changes from being done to authorized applications, like DLLs, system files, registry.				**On-premises**
23	The solution should be able to work in monitoring as well as blocking mode.				**On-premises**
24	The solution should give granular control to block versions lower than a particular version of an application.				**On-premises**
25	The solution's management console should have the				**On-premises**

	capability for separation of functions and access by roles				
26	The Solution should be capable to deploy the policies in scheduled process or real time basis.				**On-premises**
27	The Solution Should Allow or block applications using a score generated by the Threat Intelligence inputs.				**On-premises**
28	Solution Should Match Certified Safe Software and endpoint inventory applications dynamically.				**On-premises**
29	Solution should support Permanent Trusted Level-Allows applications that match this rule to install and start any other applications				**On-premises**
30	Solution Should support all the Browsers and their versions (admin need not find all dll/sha/path himself).				**On-premises**
31	Solution should support automatic intelligence of well-known applications and versions for Developer tools (admin need not find all dll/sha/path himself).				**On-premises**
32	Solution should support automatic intelligence of well-known applications and versions for Distributed Computing (admin need not find all dll/sha/path himself).				**On-premises**
33	Solution should support automatic intelligence of well-known applications and versions for Encryption (admin need not find all dll/sha/path himself).				**On-premises**
34	Solution should support automatic intelligence of well-known hardware and Firmware drivers (admin need not find all dll/sha/path himself)				**On-premises**

35	Solution should support automatic intelligence of applications and versions for High-Risk Applications like Key Loggers, Proxy anonymizers (admin need not find all dll/sha/path himself)				**On-premises**
36	Solution should support automatic intelligence of applications and versions for all well-known Media tools like Adobe (admin need not find all dll/sha/path himself)				**On-premises**
37	Solution should support automatic intelligence of applications and versions for MS Applications and capable to restrict users to a certain version(admin need not find all dll/sha/path himself)				**On-premises**
38	Solution should support automatic intelligence of applications and versions for Productivity tools like Adobe, (admin need not find all dll/sha/path himself)				**On-premises**
39	Solution should support automatic intelligence of applications and versions for System applications like Download Managers, File Compression, Server Services, Software updaters (admin need not find all dll/sha/path himself)				**On-premises**
40	Solution should have capability to set up approval workflow and workflow for exception.				**On-premises**
41	The Solution should maintain Version Control of at least 5 changes addition/deletion/modification).				**On-premises**
42	Should have the ability to enforce either Block or Allow unrecognized software. Solution should be capable of creating whitelist for each				**On-premises**

	server dynamically and no manual intervention in creating this list.				
43	Solution must support Lock Down mode: No Software is allowed to be installed except what is detected during agent installation.				**On-premises**
44	Solution must support Global Blocking on the basis of Hashes/signature or any other method and create blacklist for the environment.				**On-premises**
45	Solution should be capable of whitelisting applications & software on servers & desktops. It should also block unauthorized executable files, libraries, drivers, scripts, and specialty code on servers and desktops.				**On-premises**
46	Solution should have option to allow to install new software or update by setting up maintenance mode				**On-premises**
47	The application control component must have in built capability to detect, notify and (if required) prevent older version of the applications from being executed.				**On-premises**

(D) FILE INTEGRITY MONITORING FEATURES

Presently, Bank is using both windows and non-windows based operating systems for various financial and non-financial application servers to perform day to day business activity. Bank requires a File Integrity Monitoring (FIM) module in new ESS solution. FIM is important for Windows-based environments as well as non-windows environments Linux/UNIX systems and other available OS systems. Windows uses the registry for most of its configuration, combined with the Win32 API, which is a tightly controlled and restricted area. In Linux and UNIX environments, configurations are much more exposed as part of the overall file system. FIM module is expected to have features like scan, analyze, and report on unexpected changes to important files in our IT environment for Detecting illicit Activity, Pinpointing Unintended Changes, Verifying Update Status and Monitoring System Health and Meeting Compliance Mandates. FIM functionality can also be carried out on a continual, snapshot, or regular basis. Bank requires FIM module which

act as broader auditing and security solution that will also include capabilities such as automated rollback of changes to an earlier, trusted state. FIM solution will provide clear and rapid information on who, what, where, and when for every access and change event in endpoints of Bank. Presently, Bank requires FIM module for servers only. Bank may implement the FIM on endpoints other than servers, if required. All cost included in Project cost. No extra cost will be paid during contract period. FIM module should check under mention specification of File based monitoring as under:

Sr. No.	**Specifications**	**Compliance with clear /explicit Supporting Documents** (Yes/No)	**Available as part of OEM solution** (Yes / No)	**To be made available as Customization or Third Party** (Yes / No)	**Feature availability (on Cloud/On-premises /Both)**
1	The proposed solution should provide an option for real time or scheduled Integrity monitoring based on operating system.				**On-premises**
2	Solution should support automatic creation of baseline to identify the original secure state of the monitored server to be compared against changes.				**On-premises**
3	Solution should have an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features.				**On-premises**
4	Solution should support Multiple groups of hosts with identical parameters, Regex, or similar rules to define what to monitor, Ability to apply a host template based on a regex of the hostname,				**On-premises**

	Ability to exclude some monitoring parameters, Ability to generate E Mail and SNMP alerts in case of any changes, Solution should support creation of custom Integrity monitoring rule.				
5	Solution should support tracking of Created, modified, and accessed settings and permissions.				**On-premises**
6	Solution should support to keep track of Security and privilege settings modified on files.				**On-premises**
7	Solution should support to keep track for change in Content of the file.				**On-premises**
8	Solution should support to keep track for Core attributes and size.				**On-premises**
9	Solution should support to keep track of changes in Hash/signature values based on file contents.				**On-premises**
10	Solution should support to keep track Application, Databases, directories, OS, and middleware.				**On-premises**
11	Solution should support to support file systems for Multi-platform and have Centralized control for appropriate action.				**On-premises**
12	Solution support differentiation between positive, neutral, and negative changes and Advanced and Flexible Reporting.				**On-premises**
13	Solution should be capable in Prevention of changes to				**On-premises**

	critical files related to OS and Databases.				
14	Solution should be Capable of supporting different policies according to the device type. Ability to revise a policy according to Banks's individual requirements. All endpoints should quickly update via content downloads.				**On-premises**
15	Solution should be Capable of supporting change management, Threat Detection, and audit compliance for Bank's ISD, HIPAA, FISMA, NIST and PCI DSS. Real Time monitoring and Simplified Rule configurations.				**On-premises**
16	The solution should support all available versions of Windows & non-Windows servers.				**On-premises**
17	The solution should support available databases like Microsoft SQL, NOSQL, Oracle, MySQL, and MongoDB.				**On-premises**
18	The solution should have the capability to provide integration with existing user management systems e.g., Active Directory and have built-in identity management capabilities. Such integration should be part of on premise /hybrid cloud configuration also.				**On-premises**
19	The solution should support API integration with on premises Single Sign On systems, external authentication systems (like MS Azure AD).				**On-premises**
20	The solution should have the capability to allow enforced watermarked viewing of protected files				**On-premises**
21	The system administrator should be able to define and				**On-premises**

	control which users are allowed to define policies and can monitor these policies for compliance to the Bank's security standards. Admin/Owner of the File Contents should also be able to transfer File Content ownership.				
22	The solution should be capable to provide web-based activity searching and reporting of user activities and admin activities				**On-premises**
23	The audit trail should capture the person who has used the File-content, what has been done (un/authorized), the time, and the location. Activities can be exported to be consumed by other monitoring systems.				**On-premises**
24	The File Integrity Monitoring is proposed to be a module of overall ESS Solution which should be easy to configure, provide offline access also to protected File contents.				**On-premises**
25	The solution must be easy to use and must support integration with existing enterprise applications.				**On-premises**
26	The solution should be capable to allow for automated folder-based protection for Bank's servers. All files must be automatically protected with predefined policies.				**On-premises**
27	The solution's configuration / updates and upgrades must be easily manageable by the IT team of the Bank				**On-premises**
28	The solution should be capable to support delegation of duties and administrative functions for efficient management by various IT-Application Owners.				**On-premises**
29	The solution should have minimal or no dependency on other proprietary hardware/				**On-premises**

	software on the desktop or server				
30	The solution should not cause conflicts with other security systems like anti-virus, anti-malware systems				**On-premises**
31	The solution should support segregation of duties (defining end users, system administrators, policy administrators).				**On-premises**
32	The solution should have capability to create and apply custom FIM (File Integrity Management) Rules at organization level, department level, Group level or user level or any specified level as per requirements.				**On-premises**
33	Integrity Monitoring module should be capable of monitoring critical operating system and application elements, files, directories, registry keys to detect suspicious behavior, such as modifications, or changes in ownership or permissions.				**On-premises**
34	Solution should be able to monitor System Services, Installed Programs and Running Processes for any changes.				**On-premises**
35	Solution should have extensive file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size).				**On-premises**
36	Solution should be able to track addition, modification, or deletion though various OS log attributes.				**On-premises**
37	Solution should support configuration of any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, databases.)				**On-premises**

	and support custom rules as well.				
38	Solution should have automated recommendation of integrity rules to be applied as per Server OS and can be scheduled for assignment/assignment when not required.				**On-premises**
39	Solution should have by default rules acting at Indicators of Attacks detecting suspicious/malicious activities. Solution should have complete functionality of file integrity monitoring.				**On-premises**
40	In the Event of unauthorized file change, the proposed solution shall report reason, who made the change, how they made it and precisely when they did so.				**On-premises**
41	Solution should have Security Profiles which allows Integrity Monitoring rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required. Rules should be Auto Provisioned based on Server Posture.				**On-premises**
42	It should be capable to monitor user behavior and track changes to files and registry keys. It should also be capable to identify who made changes and to which files.				**On-premises**
43	The complete history of the changes made up to minimum 50 versions (copies of files) / up to minimum of 90 days with complete audit trails.				**On-premises**
44	The solution should be capable of comparing misconfigurations in real time against Bank's internal				**On-premises**

	standards for compliance and security best practices.				

(E) INTEGRATION OF ENDPOINT PROTECTION PLATFORM WITH OTHER APPLICATIONS / SOLUTIONS:

Sr. No.	Specifications	Compliance with clear /explicit Supporting Documents (Yes/No)	Available as part of OEM solution (Yes / No)	To be made available as Customization or Third Party (Yes / No)	Feature availability (on Cloud/On-premises/ Both)
1	Solution should have capability of integration with • Active Directory Services. • Privilege Integrity Management Systems (PIMS). • Network Access Control (NAC) and NTP (Network Time Protocol). • IT Asset management ITAM. • Security incident management SIEM, DAM and Bank SOC solution. • Bank's Proxy solution. • Firewalls, IDS, IPS for Threat Intelligence.				**On-premises**

(F) MIS AND REPORTING REQUIREMENTS:

Sr. No.	Specifications	Compliance with clear /explicit Supporting Documents (Yes/No)	Available as part of OEM solution (Yes / No)	To be made available as Customizatio	Feature availability (on Cloud/On-

				n or Third Party (Yes / No)	**premises /Both)**
1	Solution should support centralized MIS and Real time Dashboards to application owners, circle coordinators and central Endpoint Security Solution Team.				**On-premises**
2	Solution should support MIS Dashboard through OEM's software. In case, the reports and dashboards are not available as per the Bank's requirement in OEM's console, then selected bidder has to make it available through reputed / popular MIS tools available in the market at no extra cost to the Bank. It will be the responsibility of the selected bidder to manage, maintain AMC / licenses during the contract period for MIS tool.				**On-premises**
3	The centralized management console should deliver security threat information including current threats and if possible future threats also.				**On-premises**
4	The solution should support Web Services if it is required to export data out to other custom reporting solutions. Reports should be in various formats including HTML, PDF, Excel, Word, or any other feasible reporting formats. Also it should be configurable based on information required and duration.				**On-premises**

5	Solution should support customized reports or specific reports and sending them over email to be configured email ids at schedule interval.				**On-premises**
6	Solution should provide a report on list of machines where scheduled scans not completed or outdated systems for a defined time period. It should also provide reports for top 10 virus infected systems Bank wise/ group-wise/ IP Address infected endpoints.				**On-premises**
7	The reporting module of Solution should provide management reports for different managed components like- Top N reports, Trend Reports, Outbreak reports, Compliance reports and daily standard/ Customized Reports if required.				**On-premises**
8	Solution should provide a report on threat statistics to keep threat security up to date and also to pinpoint the most common entry points and monitor antivirus policies to prevent infections				**On-premises**
9	Solution should provide detailed reports for the update, upgrade, and product coverage summary with the details of the endpoints, Server (Name of the System, IP Address, MAC Address, Username, and the operating system of the Server).				**On-premises**
10	Solution should provide Bank-wise, Circle-wise/ Country-wise as well as Consolidated Dashboard which provides AV				**On-premises**

	position in the Bank. It includes update ratio, online, offline systems, granular details of non-updating systems.				

NOTE:

If bidder is able to propose a technical feature for implementation On-premises and Cloud, both, then the Bank may decide deployment of such feature in on-premises or on cloud deployment. The bidder should comply with all security controls, while proposing deployment of such features. .

TECHNICAL EVALUATION PROCESS & SCORING METHODOLGY

1. The objective of technical evaluation and shortlisting of the bidders is to facilitate the selection of the most optimal Solution(s) that appropriately meet the requirements of the Bank. All bids shall be evaluated by an evaluation committee set up for this purpose by the Bank. The Bank will evaluate the technical offers of the bidders complying with Eligibility Criteria mentioned in the Appendix-B and the proposals meeting the said criteria will only be taken up for further technical evaluation.

2. As part of the technical bid, the bidder shall have to submit all the specified documents/information covering all the clauses specified in the RFP. The Bidders shall be required to deliver an exclusive presentation detailing the proposed architecture and implementation approach, rollout strategy for the proposed ESS solution. Due to the ongoing COVID-19 pandemic, bidders may be requested to present their solution through online mode. The details of the online presentations will be shared with the bidders at an appropriate time.

3. The bidders are expected to submit a soft copy of the presentation to the Bank along with their technical and commercial bids.

4. A bidder will qualify the technical evaluation stage by scoring a minimum of 75% of total marks. Based on the scores, qualified bidders shall be shortlisted for further participation in the RFP process. The decision of the Bank in this regard will be final.

5. A Bidder needs to achieve a minimum score of 75% marks in this evaluation stage to be qualified for commercial bid opening. Only those vendors who achieve a minimum score of 75% marks would be short-listed for Commercial Bid Evaluation. The Technical Proposal will be evaluated for technical suitability based on following criteria

6. Bidder’s presentation should cover following aspects:

Sr. No.	Evaluation of Bidder's presentation
1	Project plan and Execution Methodology
2	Solution Architecture and Design – Key Features and Functionalities
3	Meeting with Bank's User Acceptance Criteria and information Security Requirements.
4	Compliance to CERTIN, RBI, CSITE, and Bank's Security and other Regulatory guidelines.
5	Implementation and Operational aspects and Adherence to Project Timelines

7. The presentations would be delivered to a competent panel chosen appropriately by the Bank for the purpose of technical evaluation. The evaluation process for shortlisting of the bidder will be based on the evaluation matrix given below:

TECHNICAL EVALUATION MATRIX

Sr. No.	Criteria	Max. Marks	Scoring	Bidder Response
1	Number of projects executed by the Bidder in last 3 years for implementation and maintenance of "Endpoint Security Solution (ESS)".	10	➢ 3 or more projects – **10 marks** ➢ 2 projects – **07 marks** ➢ 1 project – **05 Marks**	Relevant verifiable certificate to be submitted.
2.	The proposed solution with number of Endpoints covered as a single installation. Principal organization will be considered as single installation.	10	➢ Endpoints above 2,00,000 – **10 marks** ➢ Endpoints 1,00,001 to 2,00,000 – **8 marks** ➢ Endpoints 50,000 to 1,00,000 – **5 marks** ➢ End points less than 50,000- **0 marks**	Relevant verifiable certificate to be submitted.

3.	Number of Servers covered as a single installation for implementation and maintenance of "Endpoint Security Solution (ESS)"	10	➢ Servers above 20,000 – **10 marks** ➢ Servers 10,001 to 20,000 – **8 marks** ➢ Servers 5,001 to 10,000 – **5 marks** ➢ Servers less than 5000 – **0 marks**	Relevant verifiable certificate to be submitted.
4.	OEM should be empaneled with the Ministry of Electronics and Information Technology (MeiTY).	5	➢ **Compliant** – 5 marks ➢ **Non-compliant** Technically disqualified	Relevant verifiable certificate to be submitted.
5.	OEM cloud or its designated cloud service provider should be ISO-27001 & ISO-27017 or Global SOC2 compliant.	5	➢ **Compliant** – 5 marks ➢ **Non-compliant** Technically disqualified	Relevant verifiable certificate to be submitted.
6.	OEM's and Cloud Service Provider's (CSP) data centers should be minimum Rated 3 of TIA940 or Tier 3 of 'Uptime Institute' or any other equivalent certification.	5	➢ **Compliant** – 5 marks ➢ **Non-compliant** Technically disqualified	Relevant verifiable certificate to be submitted.
7.	The OEM and Cloud Service Provider's (CSP) data centers should be PCI-DSS compliant for any credit card or debit card data is processed/stored or involved in any manner,	5	➢ Storing / processing and PCI-DSS compliant **– 5 marks** ➢ Not Storing / not-processing and PCI-DSS compliant **– 5 marks** ➢ Not Storing / not-processing and PCI-DSS non-compliant **– 5 marks** ➢ Storing / processing and PCI-DSS non-compliant **technically disqualified.**	Relevant verifiable certificate to be submitted.

8.	Compliance with the technical requirements mention in Appendix-C EPP & EDR =221 ACC =47 FIM=44	20	➢ 100% compliance with the technical requirements mentioned in each (section A, section B, section C, section D and E) of Appendix-C at the time of bid submission – **20 marks** ➢ **Non-compliant** Technically disqualified.	
9.	**Proposed feature Percentage i.e. Cloud %, On-Prem %** (Total 221 features covering EPP & EDR will be considered as 100%)	10	➢ Proposed solution having Cloud features percentage between 60% to 40% and corresponding On-Prem feature between 40% to 60% – **10 Marks**. ➢ Proposed solution having Cloud features percentage between 60% to 70% and corresponding On-Prem features between 40% to 30% – **5 Marks**. ➢ Proposed solution having On-Prem feature percentage between 60% to 70% and corresponding on Cloud feature between 40% to 30% – **5 Marks**. ➢ Proposed solution having Cloud features above 70% or below 30% and corresponding On-Prem features	

			below 30% or above 70% - **Technically disqualified**	
10	Domestic verifiable Customer References for proposed ESS Solution (If bank is not able to get response after 02 attempts within one week then it will be treated as non-compliant, and no mark will be awarded)	5	➢ 03 or more references **– 5 marks** ➢ 02 references **– 3 marks** ➢ Less than 02 **references – 0 marks**	
11	Global verifiable Customer References for proposed ESS Solution (If bank is not able to get response after 02 attempts within one week, then it will be treated as non-compliant and no mark will be awarded).	5	➢ 03 or more references **– 5 marks** ➢ 02 references **– 03 marks** ➢ Less than 02 references **– 0 marks**	
12.	**Presentation**: 13. Presentation on proposed architecture with technical features readiness vis-à-vis Bank's technical specification. 14. Rollout and implementation strategy for 100% deployment within defined timelines. 15. Availability of Manpower L3, L2, L1 resources. 16. SLA compliance including (but not limited to): i. Performance Requirements ii. Scalability Requirements iii. Regulatory and Compliance Requirements not limited to Bank's Information Security, IEHRT, SOC, CERTIN, RBI CSITE advisories, response on Zero Days malwares/ threats with advance AI/ML based intelligent model	10	Evaluation by the Committee	

	having heuristics behavioral monitoring and protection capabilities to secure Bank's IT ecosystem.			
Total		**100**		

Note:

1. The above score chart contains objective parameters (from Sr. No. 1 to 11) and subjective parameters (Sr. No. 12)

2. Compliance with all the specifications mentioned above must be supported by relevant and verifiable documents. All such supporting documents must be submitted along with the technical bid.

3. Only principal organizations will be considered excluding subsidiaries and associates.

Name & Signature of authorized signatory

Seal of Company

Appendix-D

Bidder Details

Details of the Bidder

S. No.	Particulars	Details
1.	Name	
2.	Date of Incorporation and / or commencement of business	
3.	Certificate of incorporation	
4.	Brief description of the Bidder including details of its main line of business	
5.	Company website URL	
6.	Company Pan Number	
7.	Company GSTIN Number	
8.	Particulars of the Authorized Signatory of the Bidder a) Name b) Designation c) Address d) Phone Number (Landline) e) Mobile Number f) Fax Number g) Email Address	
9	Details for EMD Refund (applicable only if EMD is directly credited in designated account): - a) Account No. b) Name of account holder c) Name of Bank d) IFSC Code	

Name & Signature of authorized signatory

Seal of Company

Appendix-E

Scope of Work and Payment Schedule

Background:

The existing antivirus solution was procured by Bank in year 2010-11 and subsequently in year 2015-16, as per the Bank's procurement procedures and policies. Presently, the antivirus solution is protecting the endpoints i.e. (desktops, servers (physical and virtual)) having windows and non-windows operating systems. The management console of the existing solution is deployed in Bank's private cloud and it is operational from primary site as well as disaster recovery sites of the Bank. The scope is to Supply, Implement, integrate, test, operationalize, maintain, and support the overall Endpoint protection & Server security solution including ACC and FIM capabilities on endpoints & servers in SBI landscape during the contract period of 5 years.

Table I:

Sl No	Requirements	Particulars
1	Description of Services	1. The successful bidder has to provide detailed solution document, project implementation plan, architecture diagram (HLD and LLD) and provision for hosting the proposed solution through Bank's private cloud virtual environment or may also propose and supply their own hardware configurations (required for deployment of on-premises components of ESS solution, within fifteen days from the date of issuance of purchase order by the Bank. The solution provider should provide a detailed Plan of action (POA) for implementation of entire solution as per the RFP within 07 days of issuance of PO. 2. The solution should comply and meet all technical features as proposed in this RFP. All feature customisation, enabling, disabling, and parametrisation during the contract period to be ensured by successful bidder / OEM without any additional cost to the Bank. 3. Provision of 4,00,000 enterprises licenses from OEM for endpoint security solution by successful bidder. 4. If required, the Bank may purchase additional licences (maximum 1,00,000) at the same rate as discovered in the RFP during the Contract Validity.

		5. The successful bidder has to setup Endpoint security solution infrastructure in Bank's private cloud or provide their own hardware/software at Bank's DC and DR locations. 6. Supply, installation, commissioning, and implementation of Endpoint Security Solution across the Bank, including its maintenance, administration, support, upgradation, enhancement of Server, Database and Backup administration including overall infrastructure with no additional cost during the entire contract period of 5 years. 7. Implementation and maintenance of setup at Primary and DR sites along with UAT setup at any one location. Clearance of solution architecture from Bank E&TA Dept. 8. Fixing of Comprehensive Security Review findings, after first setup and thereafter as and when carried out by Bank information security department and any other security or compliance audit findings within the prescribed time limits. Solution will be rolled out only after closure of all security findings by the Bank's Information Security Department. 9. Implementation of Endpoint security solution across the Bank on endpoints in Domestic, Foreign Offices, roaming endpoints, and Bank customer touch points such as CDK, QMS. 10. Operational support (viz. regular job execution and monitoring, server Backup/restoration, technical housekeeping, disk space, training) before and after production deployment Installation. 11. Bank proposes to use Bank's private cloud for deployment of on-premises component of the solution. However, if bidder requires any specific hardware (for on-premises components) for delivering the solution, the cost for the same to be included in the price bid. 12. Offered products / Software/hardware should be of latest version and should not have End of Life / End of Support in the next five years. 13. For all type of technical support services/premium support & SLA where involvement of OEM is required, there should be a back-to-back agreement between successful bidder & OEM, if OEM itself is not the bidder. For Bank bidder will be the single point of contact. 14. Bidder will ensure Services from the OEM to be available round the clock during the contract period.

15. Selected bidder should ensure that OEM has to release the models of machine learning for preventing the intrusion of the file and file-less malwares for which the signatures are not available. SI will be responsible for deploying these models/signature on the endpoints timely and proactively.
16. Selected bidder will be responsible for arranging the signatures from the OEM proactively as a preventive measure for the Bank, on or before the malwares are published. OEM must have intelligent network for getting original malware files and samples for releasing the signature. Bidder will be responsible for deployment of the signature on endpoint.
17. OEM should be pioneer in releasing the signatures and updates of AI&ML models proactively as and when new IT-Threats are identified, locally or globally. In case, new threats are declared and any other OEM has the remediation for these new threats, then the OEM is responsible for releasing the signature / pattern/AI&ML models within 06 Hrs, to protect the Bank from these new threats.
18. Signature/remediation for all new malware or IT-Threats must be deployed across all endpoints within 12 hours from their availability on central ESS management server's setup.
19. Bidder to provide the 24*7*365 support for Implementation, Integration, Maintenance, Administration, Onsite-Support and Licenses for Centralized Endpoint protection platform (EPP), Application Change Control (ACC), File Integrity Monitoring (FIM) and Early Detection and Response (EDR) as a comprehensive Endpoint Security Solution during contract period of 5 years.
20. Bank will provide limited virtual servers for deployment of the ESS solution with below configurations

Sl. No	Description	Core (vCPUs)	Memory (GB)	Storage (GB)
1	Web/App servers	32	64	300
2	Database Server	64	128	1000

The maximum possible layout for proposed new solution can be within ± 10% of existing infrastructure.

In case ESS solution requires high end servers, more storage, more CPU and processing power for better performance, threat analysis and forensics, bidder has to provision the hardware/software/servers along with OS and other required licensed software's at any point of time during the contract

		period of 05 years. All cost is to be included in the project cost. No additional cost will be paid by Bank for these Hardware's and software's. Bidder has to account for the required hardware, project performance including warranty, AMC and required support during the contract period within the overall cost.
2	Description of Deliverables	1. Implementation plan should be provided for roll out of the ESS on **400000** Endpoints including desktops, servers (physical and virtual) windows and non-windows, roaming clients viz mobile devices iPad, laptops, mobile and virtual servers under Branch Server consolidation (BSC) and Bank private cloud at PR & DR. ESS central management console servers will be installed in SBI premises. 2. It will be the responsibility of the selected bidder to ensure 100% communication status of Endpoint Agents and to take corrective steps in co-ordination with the Bank, to resolve agent communication issues and ensure 100% communication of endpoints with central management servers. 3. Develop a strategy to ensure 100% coverage of Bank's assets of various OS flavors and endpoints i.e. desktop, server (physical or virtual), windows, non-windows and other Operating Systems available with Bank and new OS that may be procured by Bank during contract period without any additional cost. 4. The solution should have a Report Scheduler to auto generate and distribute relevant periodic pre-defined reports to asset owner/ SPOC of departments. 5. The scope of the project also includes training & handholding to the designated staff of the Bank. 6. The software / hardware / licenses / AMC / management / maintenance / developer / warranty / VAPT / patching will be responsibility of the bidder during the contract period of 5 years. 7. 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. 8. The scope of the project also includes Server hardening as per Bank's Secured Configuration Document, closure of VA observations, maintaining Secure Configuration Documents

		and configurations of necessary key stores and certificates wherever required. 9. The Bidder shall provide hardware sizing of the solution (on-premises components) to ensure that the capacity utilization including memory, CPU, Hard disk space should not exceed 60 percent. During the period of contract, a periodic review of the solution size to be undertaken, and report shall be provided to ensure the resource utilization is below 60%, at all times. 10. 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. The bidder should also ensure that the latest versions recommended by ISD/OEM of all the components in the solution are configured in the production at any point of time during the contract period. 11. The delivered solution should ensure scalability as per Bank's requirements and ensure immediate response to the end users. 12. The Bidder shall perform the periodical Backup, load testing and backup restoration activities of the solution and ensure that the immediate restorable version of the solution is available maintaining the data integrity. 13. Provide updates and upgrades of the product during the entire contract period, at no additional cost to the Bank. 14. The solution must be able to detect/block/quarantine/clean the files/IT-threats for the hashes and IOC/IOA released by RBI/Cert-in/any other regulatory bodies in India and abroad through its agent on endpoint OR OEM has to provide the dedicated scan engine for detection/clean of these hashes and IOC/IOA released by advisories. The solution must be compliant to detect/block/quarantine/clean all the alerts and advisories released by RBI/Cert-in/any other regulatory authority in India and abroad in past also at the time of implementation/rollout of the solution. Bank will not provide any information related to advisories/alerts released by the various regulatory bodies in India and abroad. Bidder has to arrange through OEM and provide confirmation of the resolution to detect/block/quarantine/clean all the alerts and advisories released by RBI/Cert-in/any other regulatory authority in India and abroad during the contract period. Bank will not pay any additional charges for this activity. It is included in total project cost. 15. Bank requires a comprehensive endpoint security solution (ESS). It the responsibility of the Bidder/Service integrator to

		share each and every requirements of the Bank mentioned in RFP with OEM, to make them equally responsible for delivery of the solution as per Bank requirement. 16. As the technical specifications, features, modules required by Bank in ESS solution, will be delivered by the OEM, bidder can share the RFP with OEM for better understanding of the Bank's requirement. It is the responsibility of the bidder to sign a SLA with OEM and confirm to the Bank on the similar lines to this RFP to ensure end to SLA terms. 17. OEM is responsible to release the detection for alerts released by RBI cert-in and any other advisories from India or foreign location proactively. 18. Bidder is responsible for follow-up with OEM and arrange the latest signature/patterns to the SBI in case any malware/ransomware/ alert released by advisories in India or any other foreign countries. 19. Bank will not provide the malware or malicious file for creation the signature or detections 20. As per Banks requirement, Bank will arrange the dedicated link for connectivity between Bank's On-premises ESS infrastructure and OEM Cloud/Data center for both DC & DR setup. Further, Bidder is responsible for providing network devices like (router, switch) and any other devices required for connectivity for redundancy on DC & DR location of Bank and OEM cloud. Bidder is also responsible for monitoring link uptime, networking device management, maintenance and administration. 21. Bank has right to check and verify the deliverable in RFP at any point of time during contract period of 05 years by SBI officials or any other third party organization assign by Bank for verification of the deliverables in RFP. In case of any feature/functionality/deliverables is missing or not delivered then Bank will impose penalty or take action accordingly.
3	Third-Party Components	1. Hardware, software or any third-party items and materials included in order to provide Endpoint security solution along with EPP, EDR, ACC, FIM capabilities, MIS tool OS and DB administration are part of the deliverables during the contract period without any extra cost to Bank. 2. The Bidder shall be responsible of all technical activities like VA, patching, upgrade and updates troubleshooting, included but not limited to licensing and configuration of all the third-party components provide along with the solution without any extra cost to Bank.

4	Term of the Project – Project Schedule; Milestones and delivery locations	1. Project Schedule and milestone: As per SLA Appendix-J. 2. Delivery Locations: Helpdesk support at SBI, GITC, CBD Belapur. 3. Software at Bank's Data Centre at Navi Mumbai, and Hyderabad. 4. The Bank may shift the Endpoint security solution infrastructure to any other location decided by Bank during the contract period. 5. The project delivery schedule / timelines are as given in the Table II.
5	Integration / Migration Requirements with existing systems.	1. The proposed solution should work along with the existing Antivirus till the completion of implementation/migration and in production of new Endpoint security solution. After migration to new ESS solution, Service Integrator also ensure for removal of OLD antivirus solution from end points and servers. 2. Integration with Banks firewall where firewall policies can be implemented which blocks active Command & Control (suspicious network intelligence) attempts communication attempts identified by the solution. Also, integration with Bank IDS & IPS. 3. The Bidder to build the service catalogue for the support team to ensure smooth services to all the end users. 4. All the systems/components in the proposed solution should be integrated with the Bank's current security and IT operation systems like SOC, PIMS, DLP, AD, ITAM, NAC, NTP and all such security and operations management systems which will be deployed in the Bank from time to time. 5. **Web Proxy Integration:** Integration with web proxy where web access policies can be implemented based on state of the endpoint (suspected or infected) discovered by the solution. Integration with web proxy where web access policies can be implemented which blocks active C&C communication attempts identified by the solution 6. **NAC Integration:** Integration with Network Access Control (NAC) solution. 7. **NTP (Network Time Protocol):** Integration with NTP Server of the Bank. 8. **Active Directory Integration:** Integration with Active Directory AD solution. 9. **PIMS Integration:** Integration with Privilege Identity Management solution (PIMS) of the Bank for accessing the endpoint security solution infrastructure servers.

		10. **Bank SOC SIEM and DAM integration:** Integration with SIEM and DAM solution in the Bank. 11. **Email Integration:** Integration with Bank's Email Solution, Office365, create / add identified threats file integrity hash value. The Solution can work in conjunction with Office365 suites, but it should not be dependent on it.
6	Help Desk Requirements	a) Onsite Helpdesk support **(24*7*365)** facility during the contract period of 5 years. b) Onsite team shall be responsible for application and database administration, daily technical housekeeping activities, patching, update/upgrade, configuration management, monitoring, integration, fine tuning, and any other technical support for the complete solution including third-party solutions if any, provided to the Bank. Overall application availability, health and performance monitoring will be part of the responsibility. c) The expected time of resolution should be average 30 minutes per call. d) Policy configuration/customization as per requirements of the Bank's governance policy regularly. e) Bidder must do first level of checking / examine / interview / verification and then recommend the suitability of the resources (L1, L2, L3, Team lead and MIS manager if any.) in project. Bank reserves the right to interview all the professionals to be deployed in the project and reject, if not found suitable. At a later stage also, if any of the professional found unsuitable or incapable or violates any of the bank guidelines Bank may ask to remove all such professionals at a short notice f) The resources will be on-boarded after scrutiny as per the Bank's requirements and bidder has to submit the necessary documents within 5 days to Bank for generating the access card. g) Properly laid down escalation matrix clearly stating the L1, L2 and L3 support structure. h) Support the end-users and departments in the pre and post deployment during contract period. i) The expected time of resolution should be average **30** minutes per call. j) Escalation process should be in place for unresolved issues *k)* Helpdesk staff should be well trained to effectively handle administration, maintenance, management, and operational support/queries raised by the Bank's other IT application department / end users.

		l) Helpdesk Resources should have ability to generate MIS reports periodically for example: Number of systems up to date, number of systems not updated systems at Bank level, Volume of calls / per day, resolution % per day. m)The bidder has to maintain educational qualification and experience requirements of the resources in the project. Any deviation in the educational/qualification of the resources is only under Bank discretion. n) The Bidder shall help the bank in reducing overall incidents and false positives. *o)* Any incidents shall be notified to the designated stakeholders and resolution of such incidents shall be resolved without any delay. *p)* The successful Bidder has to provide throughout the contract period, the services of **02 (Two)** onsite Technical resource (L3) employee of OEM, onsite **06 (Six)** number of L2 Engineer, **35 (Thirty Five)** number of L1 Engineers at GITC Belapur and Banks LHO, Corporate Office with the qualifications and Experience as defined below: **1. Key Personnel: Technical Resources (L3)** • Graduate Engineer Computer Science/IT/MCA with minimum 5 years of experience or BCA/B.Sc.-IT/BSC-Computers with minimum 8 years of Experience in implementing, managing, and troubleshooting large size Endpoint Protection/EDR/Threat Hunting/Forensics with at least 10,000 endpoints in single installation. L3 must have complete product knowledge. • Sound knowledge of Endpoint security solution solutions, E-Mail, Network APT /EDR/ACC/FIM /Threat Hunting/Forensics architecture, product function, features pertains to proposed ESS solution and its equivalent security solution. • Proven track record on trouble shooting the E-security solutions issues. Certified L3 level Specialist with any reputed Endpoint Protection/EDR software, Next-Gen antivirus products organization Certified certification. 2. **L2 – Engineer's Qualifications**: • Graduate Engineer Computer Science/IT/MCA with minimum 3 years of Experience or BCA/B.Sc.-IT/BSC-Computer with minimum 5 years of Experience or B.Sc./B. Com/Diploma in Computer science/IT with

		minimum 6 in Experience in Support and implementation of Security Products including antivirus solution, Endpoint Protection E-Mail, Network APT /EDR/Threat hunting/Forensics Solutions. • Good Knowledge on Linux & Windows operating systems, Databases, Network Management Software and IT technologies. • Having L2 certificate of any reputed Antivirus Software solution, Endpoint Protection Platform /EDR/ACC/FIM /Threat Hunting/Forensics product features known as certified security expert. 3. **L1 – Engineer's qualifications**: • Graduate Engineer/GNIIT/MCA/BCA/B.Sc.-IT/BSC-Computers with minimum 1 year of Experience or B.Sc./B. Com//Diploma in computer science or Information Technology with minimum 1.5 years of Experience in Antivirus solution, Endpoint Protection E-Mail, Network APT /EDR/ACC/FIM/Threat Hunting/Forensics solutions. • Trained on Help Desk Operations Management. Desirable Certified as Endpoint Protection Platform/EDR/Threat Hunting/Forensics, antivirus solution handling technician. Number of L3, L2 and L1 engineers at GITC Belapur for providing 24x7x365 support services is as under: Technical Resources: **02** number of L3 Engineers of OEM will be placed at GITC and should be present 08 Hrs. x 6 days in week in 02 shifts for providing uninterrupted service for contract period of 5 year. However, L3 should be available anytime as and when required. L2- Engineer: **06** number of L2 Engineers will be placed at GITC and should be present 8 hrs. x 6 days in week in 03 shifts for providing uninterrupted services contract period of 5 year. However, L2 should be available anytime as and when required. L1- Engineer: **17** numbers of L1 Engineers will be placed at GITC and should be present 24x7x365 days basis for providing uninterrupted services round the clock. Team leader will be

		responsible for submission and maintaining of weekly roster and uninterruptable service to the Bank. L1- Engineer: **18** numbers of L1 Engineers will be placed at Banks respective LHO, Corporate Office and should be present 8hrs x 6 days basis for providing uninterrupted services on all working days. The no. of resources may very or redeployed to above any office as per Bank requirement. Successful bidder should advise name of the Team Leader who would be single point of contact for the Bank and would be responsible for managing day to day activities like relief arrangement for GITC, shift duty, arrangement of Endpoint security solution Helpdesk, training for SPOC, deployment of SPOC at different locations, Preparation and putting up of the various daily/weekly/monthly reports to the SBI Team and other administrative and MIS related work pertain to ESS solution. Bidder should also provide the escalation matrix to resolve high level technical/operational/administrative issues for successful execution of Endpoint security solution project in the Bank. Successful Bidder has to arrange relief arrangements for resources on leave for more than 03 days. Note: The suitability of the L1 & L2 engineers will be decided by the Bank before inducting the L1, L2 engineers in the Endpoint Protection Platform/EDR Helpdesk support operations. The Bank reserves the option to interview the proposed SI resources before onboarding. System Integrator has to arrange the system administrator (Linux, windows) /database administrator's (Oracle, MSSQL and any other DB used in proposed ESS solution.) or any type of software's used in Endpoint security solution provided, if any required during the contract period for resolutions of issues. Bank will not pay any extra charges for such adhoc arrangements.
7	MIS Report Generation requirement and Documentation	a) User-defined reports should be provided as per requirement of the Bank. b) Report can be generated Circle wise, Zone wise, Top & performance Report, Trend report and any other standard reports. as well as customized reports for better MIS and management. c) The solution should provide reports such as: - Executive Reports - Incident Response Reports

		- Infected and outdated System Reports - Malware/threat in Motion Reports - System Health Reports -Other customized reports as required by Bank - Reports and logs for Audit Trails. - Reports as per the requirements of the regulators and compliance authority. d) Specific / custom reports will have to be provided within 01 day from the time of request raised by Bank. e) If required, the bidder may arrange any other reputed MIS tool for fulfilment of reports and dashboards, Bank will not pay additional cost for the same. f) An indicative format of various reports required is given in the Table III. **Dashboards:** a) The solution should have a dashboard providing license deployments for all components, security settings, performance and other relevant information's pertains to proposed ESS solution. b) A single dashboard should be available for enterprise view of security posture and should have customizable dashboards and role-based admin facility. c) Must have an intuitive graphical User Interface (GUI). d) 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. e) Dashboards may be provided through Endpoint security solution console or any other recognized/reputed MIS Tool at no extra cost to Bank. **Documentation:** Bidder has to provide documents /SOP/ Manuals and other documentations as and when required by the Bank as per standard format or any specific format of the Bank during the contract period. An indicative list of the documents is as below: a) Solution architecture. b) Project plan with milestones, resourcing, and deliverables. c) Architecture & design (HLD, LLD) document including network architecture, traffic flow document between the devices. d) SOP documents. e) Product literature, Operating manuals f) Documentation on troubleshooting.

		g) Infrastructure build document. h) Application upgrade and patch management document. i) Testing cases and test results documented before and after implementation. j) Industry best practices, use cases and customization for SBI k) Vendor support details and escalation matrix. l) OEM support details and escalation matrix. m) Inventory list consisting hostnames, make, model, serial number. n) BCP plan and documentation. The above list is indicative, and the bidder has to provide customized reports and documents as required by Bank.
8	In case of Transaction System	**Audit trail requirement** a) 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 05 years. b) 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. c) Logs Integration – d) In case of Material Workload, all logs of assets related to Bank's subscription/ tenant should be integrated with the Bank's SOC. e) All logs in case of Standard Workload hosted on the cloud should be integrated with Bank's/ CSP's SOC. **Note:-Type of workload being outsourced** – The services to be outsourced to Cloud Service Provider (CSP) shall be clearly classified based on the classification of the associated data being stored/ processed/ transmitted on the cloud, as Standard Workload (non-critical) or Material Workload (critical). A Standard Workload would typically include Development and Test environments, Services not defined as 'critical'. Material Workload would include use of Critical / Sensitive data, Customer information, Staff data, that includes Personally Identifiable Information, Non-public commercially sensitive information that could influence financial markets, Regulatory reporting, or accounting data.)

9	Performance Requirements	The Endpoint security solution setup/infrastructure should maintain 99.99% uptime and RTO of 02 Hrs. Solutions must improve productivity by identifying infections automatically, reducing manual investigations of logs and alerts. A solution must be in high availability mode. Any deployed solution should provide a central installation and maintenance of client based.
10	Scalability Requirements	*a)* Solution should be scalable up to **4,00,000** endpoints but not limited to as per Bank's future requirement. b) The solution should protect 2,65,000 plus desktops endpoints. c) Windows Physical servers 10,000. d) Non-Windows Physical Servers 10,000. e) Virtual servers 68,000. f) Bank's own private cloud Setup 15,000. g) VPN laptops, Bank's laptops, and iPads. 30,000. Above mention number of endpoints are indicative. The Solution shall allow the upscaling of installations as necessary to upgrade scanning capacity with growing needs. The solution should support scalability to support large and geographically separated infrastructure to be managed centrally without having to replace software and only via addition of relevant modules. If any required. The solution sizing should be done considering the capacity details provided in the technical requirements.
11	Regulatory / Compliance Requirements	The OEM/SI and their proposed Endpoint security solution should comply all the regulatory/compliance requirements as per Bank's IS policy. Must support Policy Scan's - PCI-DSS, PA - DSS, RBI Other regulatory guidelines/standards, with custom policy /rule tweaking ability. The solution shall be compliance to all the guidelines issued by RBI, Cert-In, Bank ISD or equivalent organizations. The bidder has to provide patches and fixes for all the regulatory and audit compliance requirements and observations during the contract period without any additional cost to the Bank. The solution must be compliant to detect/block/quarantine/clean all the alerts and advisories released by RBI/Cert-in/any other

		regulatory authority in India and abroad in past at the time of implementation/rollout of the solution. Bank will not provide any information related to advisories/alerts released by the various regulatory bodies in India and abroad in past. However, if Bank provides such details to the bidder, the same should be implemented within the defined SLA timelines of this RFP.
12	Security Requirements	The Bidder should comply with Bank IT and Bank's IS Security policy in key concern areas relevant to the RFP Appendix-B1. Some of the key areas are as under: Responsibilities for data and application privacy and confidentiality Responsibilities on system and software access control and administration Custodial responsibilities for data, software, and other assets of the Bank being managed by or assigned to the Vendor Incident response and reporting procedures Password Policy of the Bank. Data Encryption/Protection requirement of the Bank. Digital forensic readiness of the solution. Comply with all the recommendations / close all the vulnerabilities reported in the various security review, IS audit, UAT and other audits conducted by the Bank, regulators, Bank appointed third parties at various stages during the contract period without any additional cost to the Bank. The Bidder shall meet all the security requirements of the Bank during the entire period of the contracts.
13	System Integration Testing and User Acceptance Testing	System Integration Testing and User Acceptance Testing. After integration and implementation of the proposed solution, the bidder shall be required to perform User Acceptance Test and demonstrate all the functionalities, required as per this RFP and contract document of the proposed solution. The Acceptance Test shall be carried out jointly by the representatives of the SBI, System Integrator and the respective

		OEM, after the proposed solution is configured and operationalized at each of the Site. A comprehensive "User Acceptance Test Plan (UAT)" document shall contain various aspects of the 'User Acceptance Test' to demonstrate all the features of the proposed solution, as envisaged in this tender document and claimed by the bidder. The User Acceptance Test shall be deemed to be complete only on the issuance of the 'User Acceptance Certificate' by the SBI to the Bidder. Without limiting the scope of the User Acceptance Test, the test cases to be carried out in this connection should be submitted by the OEM/bidder to the Bank, and subject to approval of the Bank, shall be used to assess the acceptability of the proposed solution. On evaluation of the User Acceptance Test results and if required in view of the performance of the proposed solution, as observed during the User Acceptance Test, the Vendor shall provide necessary solution at his own cost thereof, to ensure the performance of the proposed solution is meeting the requirement, as envisaged in this document. The solution provided by the Bidder must meet all the technical and other specifications at the minimum, as envisaged in this document. The Bidder shall demonstrate the capabilities and perform complete testing of equipment, features, configuration of all the equipment. The Bank will accept the "Stabilization" of the solution only on satisfactory completion of Security Audit, Validation & Certification by respective OEMs. The solution will not be accepted as complete if any facility /service as required is not available or not up to the standards projected by the Bidder in their response and the requirement of this RFP. Bank may also take up third party review of proposed feature /functionality verification at any time during the contract period for which bidder has to facilitate such third party review without any additional cost to the Bank.
14	Backup system / POC / test & training system / DR system	The bidder should provide the architecture in a way to support device wise and site wise redundancy in DC as well as DR location of Bank. Endpoint security solution infrastructure should have capacity for Active-Active or Active – Passive mode at Primary & DR site. The solution should be implemented with UAT, Pre-Prod, Production, DR instances.

		The bidder shall demonstrate the Backup and restore testing and perform quarterly planned BCP and any emergency BCP exercises.
15	Training	The bidder should provide product free training 04 times and certifications to at least **10** SBI officials each year and designated officials at OEM's R&D center.
16	Warranty and AMC of the software	The bidder has to provide necessary Annual Maintenance (AMC) during Contract period of 05 years without any additional cost to Bank.

Table II:

PROJECT DELIVERY SCHEDULE / TIMELINES:

Sr. No.	Milestone	Maximum timeline
1.	Successful bidder has to submit the project implementation plan, architecture diagram (HLD & LLD), and Virtual servers hardware configuration requirements (for on-premises components).	01 week of issuance of Purchase Order
2.	Signing of SLA, delivery of software licenses and deployment of Onsite helpdesk team resources. Delivery of Hardware by Bidders (if proposed) *or alternatively* Provision of required number and configuration of VM Servers in Bank' private Cloud setup	04 weeks of issuance of Purchase Order
3.	Installation and configuration of the solution for UAT set up.	06 weeks of issuance of Purchase Order
4.	UAT clearance and Security Review of the solution and closure of observations of security review and readiness for production setup. Helpdesk setup and manpower deployment	14 weeks of issuance of Purchase Order
5.	Production roll-out (Pilot)	16 weeks of issuance of Purchase Order

Schedule for Deployment of Endpoint Security Solution after successful closure of security review.			
Sr. No.	**Endpoints Description**	**First month of successful pilot out**	**Second month of successful pilot roll out**
1	Desktops 2.65 lakh, including CDK, QMS and Branch customer touch points.	40%	60%
2	Virtual Servers 68,000	30%	70%
3	Physical Servers (Windows & Non-Windows) 20000	30%	70%
4.	Banks Private cloud 15000	30%	70%
5.	Roaming endpoints i.e. VPN Laptops, Bank Laptops iPad, Mobile (30,000)	40%	60%

Table III:

REPORTS FORMAT (Indicative list of MIS Reports presently available)

These report formats may be considered only baseline. Bank is expecting further customization, parametrization, Secure API integration features to be made available by the proposed bidder in enhancing MIS availability for ensuring timely action taken, decision making by stakeholders, overall configuration and management of security posture compliance in the Bank.

Frequency	Report No	Report Name	Fields
Daily	D1	All export report	Circle, server, Domain, Endpoint, IP Address, Listening Port, Domain Hierarchy, Connection Status, GUID, Platform, MAC Address, Agent Program, Virus Pattern Virus Scan Engine, Agent Installation, Restart Required, Last Virus Scan (Manual), Last Virus Detection (Real-time)
Daily	D2	Outdated Agent Report	circle, server, Domain, Endpoint, IP Address, Listening Port, Domain Hierarchy, Connection Status, GUID, Platform, MAC Address, Agent Program, Virus Pattern Virus Scan Engine, Agent Installation, Restart Required, Last Virus Scan (Manual), Logon User
Daily	D3	Circle wise outdated report	circle, server, Domain, Endpoint, IP Address, Listening Port, Domain Hierarchy, Connection Status, GUID, Platform, MAC Address, Agent Program, Virus Pattern Virus Scan Engine, Agent

			Installation, Restart Required, Last Virus Scan (Manual), Last Virus Detection (Real-time
Daily	D4	Outdated AV Monitoring Sheet	Date, Count of Outdated Endpoints as on 15th of Month, Count of Outdated Endpoints as on last date of Month, Count of Outdated Endpoints as on date
Daily	D5	SPOC attendance report	Date, Location, Employee Name, Mobile No., Landline No., Present / Leave
Weekly	W1	Circle wise Offline outdated report	circle, server, Domain, Endpoint, IP Address, Listening Port, Domain Hierarchy, Connection Status, GUID, Platform, MAC Address, Agent Program, Virus Pattern Virus Scan Engine, Agent Installation, Restart Required, Last Virus Scan (Manual), Last Virus Detection (Real-time
Weekly	W2	Production	Sr No., Username, Levels, Center, Circle, Open_datetime, Callstatuscode, Description, TMCM/ OSCE/BS / Node, Close_datetime, Categorized Calls, SLA, Bank, Branch Code, Branch Name
Weekly	W3	Update Status	Date, Circle, Total Nodes (Online & Offline), Updated Nodes (Online & Offline), Update Ratio (%), Online Nodes, Updated Online Nodes, Online Update Ratio (%), Offline Nodes, Updated Offline Nodes, Offline Update Ratio (%), Online Update Ratio (%) Rank
Weekly	W4	Virus Malware report	Received, Product Entity/Endpoint, Product/Endpoint IP, Product/Endpoint MAC, Virus/Malware, Circle, Action, File, File Path
Weekly	W5	Weekly ticket count call summary	Circle , Count of Categorized Calls
Weekly	W6	MALWARE, SPYWARE INFECTED DEVICES	Circle, Count
Weekly	W7	Outdated client – circle wise	Circle, Count
Weekly	W8	Outdated server – circle wise / Dept wise	Circle, Dept, Count
Weekly	W9	FO Report	Domain, Endpoint IP Address, Listening Port, Domain Hierarchy, Connection Status, Platform, MAC Address, Agent Program, Virus Pattern, Logon User

Monthly	M1	Antivirus SLA Details	
Monthly	M2	Monthly Call Log Report	Sr No., Username, Levels, Center, Circle, Open_datetime, Callstatuscode, Description, TMCM/ OSCE/BS / Node, Close_datetime, Categorized Calls, SLA, Bank, Branch Code, Branch Name
Monthly	M3	Server down time report	Server IP , Server Hostname, Down date / time From, Down date / time To
Monthly	M4	Top 10 Infected IP report	Below Infected IP found this month, Count
Monthly	M5	Top 100 Infected IP report Frequency	IP, Count
Monthly	M6	Top 10 Virus Malware report	Received, Product Entity/Endpoint, Product/Endpoint IP, Product/Endpoint MAC, Virus/Malware User, Action, File, File Path

Roles and responsibilities of Helpdesk Team:

First level of Technical Support (L1- Support) from Bidder

1. Validation of all support cases to ensure technical issues.
2. Manage installation and configuration assistance.
3. Details / Log Information, basic level troubleshooting.
4. To know issues through OEM knowledge base articles.
5. Checking the system health in daily basis.
6. Preparing daily reports and submitting fortnightly report to the SBI/LHO/FO designated official.
7. Handling virus related calls from end users and trouble shooting.
8. Performing installation and trouble -shooting related tasks for Endpoint security solution agent.
9. Checking the Update status for all the Endpoint security solution Server and Endpoint.
10. Case logging and problem identification and Level 2 escalation.
11. Overall application availability, health and performance monitoring will be part of the responsibility. Onsite team shall be responsible for application and database administration, daily technical housekeeping activities, patching, update/upgrade, configuration management, monitoring, integration, fine tuning

Second level of Technical Support (L2 –Support) from Bidder

1. Advance or complex installation and configuration.
2. Follow up of service tickets opened on OEM.
3. Grooming Level 1 Engineers.
4. Fault isolation, case diagnosis and troubleshooting, updating operational knowledge base.

5. Any virus/ worm/spyware/malware/threat incidents reported from SBG branches/offices should be attended and a suitable solution should be provided and implemented to resolve the issue.
6. All the Endpoint security solution servers are to be kept in up and running condition.
7. Overall application availability, health and performance monitoring will be part of the responsibility. Onsite team shall be responsible for application and database administration, daily technical housekeeping activities, patching, update/upgrade, configuration management, monitoring, integration, fine tuning

Third level of Technical Support (L3 – Support) From OEM.

1. Performing analysis for day-to-day threat related calls and taking appropriate action to reduce it.
2. Single point of contact for SI and SBI /SBG.
3. Searching for new emerging threats proactively and take necessary actions.
4. To perform Configuration support, collect relevant technical problem identification information and will perform fault isolation of the problem, trouble shooting and to resolve the problem.
5. The level 3 support engineer will be responsible for monitor / manage the Endpoint security solution implemented within the SBI/ SBG Infrastructure.
6. Develop testing and deployments plans for Endpoint security solution updates and patches.
7. Will provide subject matter expertise related to end points security including virus infection and resolving it.
8. The L-3 should provide support as per SOW/SLA for any incidents reported / logged in and to resolve the issue.

The SI has to provide L-1 and L-2 support. The OEM (Product) should provide L-3 support to the Bank and System Integrator.

L-1 Support - Local engineer of System Integrator (SPOC) and or branch /office staff with the help of the SPOC try to resolve the issue. If the issue is unresolved it will be escalated to L2 Engineer at GITC.

L-2 Support - The System Integrator with their technical staff shall resolve the issue.

L-3 Support - If the System Integrator is unable to resolve the issue and is escalated to the OEM (Vendor) for their support to resolve the issue.

The process of escalation of the issue may be over phone, e-mail, web-based.

1. For the security risk issues raised by bidder to the OEM, the solution has to be provided by the OEM within 4 hours including the virus definition for zero-day virus from the time of escalation of the issue.
2. Support case resolution time

PAYMENT SCHEDULE:

The total project cost will be divided in following five components and will be paid annually as per the schedule mentioned below:

a) The Overall ESS Solution Software Licenses Cost for 05 years contract period will divided into two parts as under

i. ESS Solution Enterprise Licenses Cost.
ii. ESS Solution Licenses AMC Cost.

The 40% of the overall ESS Solution Software Licenses Cost will be paid as ESS Solution Enterprise Licenses Cost in 01st year of the contract and remaining 60% of the overall ESS Solution Software Licenses Cost will be paid as ESS Solution Licenses AMC Cost from 02nd year to 05th year of the contract. ESS Solution licenses AMC cost includes maintenance and implementation of latest ESS Solution updates, upgrades, released patches during the contract period of 05 years. The overall ESS Solution Software Licenses Cost payments terms mentioned in Table item a)

b) One Time Implementation Cost
c) ESS Solution Management & Support Cost (Onsite Helpdesk).
d) MIS Tool.
e) Hardware/Servers on OPEX Model.

The Payment schedules of various components are as follows:

a) Payment of Overall ESS Solution Software Licenses Cost during 05 year of contract		
i) Payment of ESS Solution Enterprise Licenses Cost (i.e. 40%) in 01st year of contract		
1.	Product Delivery, UAT setup, acceptance and signing of SLA	10% of Overall ESS solution software licenses cost
2.	On successful security clearance from Information Security Department of the Bank for production rollout of ESS solution. PR and DR setup.	30% of Overall ESS solution software licenses cost
ii) Payment of ESS Solution Licenses AMC cost (i.e. remaining 60%) from 2nd year to 5th year of contract.		
1.	Second Year Payment in Advance	15% of Overall ESS solution software licenses cost

2.	Third Year Payment in Advance	15% of Overall ESS solution software licenses cost
3.	Fourth Year Payment in Advance	15% of Overall ESS solution software licenses cost
4.	Fifth Year Payment in Advance	15% of Overall ESS solution software licenses cost
b) One time Implementation Cost in Arrear		
1.	Payments will be made on Monthly basis after confirmation of the implementation and submission of inventory report for implementation along with the Invoice.	Payment amount = No of endpoints implemented x Unit price for Implementation.
2.	Implementation cost for virtual servers will be included in the license cost and Payment for such licenses will be made quarterly on actual number of deployments of licenses.	Payment Amount = Unit cost of License x No of licenses deployed during the quarter.
c) ESS Solution Management & Support Cost (Onsite helpdesk)		
1.	First Year Payment in Arrears.	20% of Support Cost
2.	Second Year Payment in Arrears	20% of Support Cost
3.	Third Year Payment in Arrears	20% of Support Cost
4.	Fourth Year Payment in Arrears	20% of Support Cost
5.	Fifth Year Payment in Arrears	20% of Support Cost
d) MIS Tool (if any) Payment in Arrears		
1.	First Year Payment in Arrears.	20% of Support Cost
2.	Second Year Payment in Arrears	20% of Support Cost
3.	Third Year Payment in Arrears	20% of Support Cost
4.	Fourth Year Payment in Arrears	20% of Support Cost
5.	Fifth Year Payment in Arrears	20% of Support Cost
e) Hardware/Servers and Hardware/server AMC for contract period of 5 Year on OPEX Model		
1.	First Year payment will be in advance after delivery, installation, implementation and compliance to Bank's IS policy configurations on all server.	60% of cost of Hardware supplied
2.	Second Year payment in advance	10% of cost of Hardware supplied

3.	Third Year payment in advance	10% of cost of Hardware supplied
4.	Fourth Year payment in advance	10% of cost of Hardware supplied
5.	Fifth Year payment in advance	10% of cost of Hardware supplied
Note: Payment amount will be on actual basis on the cost of no of resources for the project required by Bank for contract period. However, the amount will be reduced, or penalties will be levied for absence of resource, if applicable as per SLA. After completion of 5 years, Bank will have the option of retaining the supplied hardware at book value or return the hardware to bidder after complying with Bank's relevant Information Security Policy at that time.		

- The penalties on account of SLA violations for OEM as well as SI support will be deducted from the invoice payments of successful Service Integrator with whom the Bank issues the purchase order and sign the SLA.
- TDS as per applicable rates will be deducted by the Bank at the time of payment of invoices.
- Bank will return the supplied hardware to the bidder after contract period of 05 year as per Banks IS policy.

[Bidder should ensure that exchange rate fluctuations, changes in import duty and other taxes should not affect the Rupee (INR) value of commercial Bid over the validity period of the bid]

Terms, Conditions for Subsidiaries/Joint Ventures

Endpoint Security Solution Infrastructure:

a. If Bank's Subsidiaries / Joint Ventures desire to implement the Endpoint Security Solution procured by the Bank, the Bank will share the rates discovered for licenses /AMC/ support /implementation in this RFP with them.
b. Domestic subsidiaries are not part of SB Connect Network, so Endpoint Security Solution infrastructure for each subsidiary will be setup by SI/OEM as per their current network architecture of the subsidiaries in consultation with each subsidiary separately as per their requirements. Hardware for their setup would be provided by them.
c. Subsidiaries and joint ventures will issue the purchase orders separately as per their requirement and payments of the invoices will also be taken care by them.
d. It is not mandatory for Subsidiaries / Joint Ventures of the Bank to implement the same solution procured by the Bank.

Appendix-F

Indicative Price Bid

The indicative Price Bid needs to contain the information listed hereunder and needs to be submitted on portal of e-Procurement agency**.** The indicative price bid will be for contract period of 05 years.

Name of the Bidder: _____

Sr. No.	**Type of services / Items (A)**	**Quantity of Licenses (B)**	**Total amount in Rs. (B) for 05 years (C)**	**Proportion to Total Cost (in percentage) #**
1.	Overall ESS Solution Software License Cost for 05 years. (includes License cost and AMC Cost)	4.00 Lakh		
2.	One-time Implementation cost for 4,00,000	4.00 Lakh		
3.	Onsite Helpdesk Support Cost for contract period of 05 years. Total 43 Resources (including L1, L2, L3)	43		
4.	Any third-party component/tool i.e., MIS tool for 05 years	NA		
5.	Hardware/servers required for delivery of solution). For 05 years	NA		
	Total Cost *			

Table-1 (Breakup of Overall ESS Solution Software Licenses Cost for 05 years)

Sl. No.	Description	Quantity as per RFP (A)	Unit cost (B)/Years	Total implementation cost (C)= (A*B*5)
1.	ESS Solution Enterprise Licenses Cost	4.00 Lakh		
2.	ESS Solution Licenses AMC Cost	4.00 Lakh		

Note: Total price of Table-1 column (C) should match with total value of Sr no.1 of Indicative Price Bid column (C).

Table-2 (Endpoint wise Breakup of License cost for Five years)

Sl. No.	Description	Quantity as per RFP (A)	Unit price of license (B)/year	Total amount of licenses for 05 Year (C) =(A*B*5)
1.	Desktops	2,65,000		
2.	Windows Servers	10,000		
3.	Non-Windows Server	10,000		
4.	Virtual servers	68,000		
5.	Bank's own private cloud Setup	15,000		
6.	Roaming clients (mobile, iPad, laptops.)	30,000		
	Above mention number of endpoints are indicative. Total	**4,00,000**		

Note: Total price of Table-1 column (C) should match with total value of Sr no.1 of Indicative Price Bid column (C).

Table-3 (Breakup of onetime implementation cost)

Sl. No.	Description	Quantity as per RFP (A)	Unit cost (B)	Total implementation cost (C)
1.	Implementation cost for 4,00,000	4.00 Lakh		

Note: Total price of Table-3 column (C) should match with total value of Sr no.2 of Indicative Price Bid column (C).

Table-4 (Resource wise Breakup of Onsite Helpdesk Team)

Sl. No.	Description	Quantity as per RFP (A)	Unit cost of resource (B)/year	Total amount of resource for 05 Year (C)= (A*B*5)
1.	L3 Engineers	02		
2.	L2 Engineers	06		
3.	L1 (Engineers at Circles, CC and GITC of Bank) 35 (17+18)	35		
	Total (1+2+3)	**43**		

Note: Total price of Table-4 column (C) should match with total value of Sr no. 3 of Indicative Price Bid column (C).

The 'Proportion to Total Cost' percentage mentioned here will have to be maintained in the final price quote also by the successful Bidder. The percentage should be mentioned in two decimal places. Variation in the final price should not exceed +/- 5%. See illustration at the end.

@ If required, the Bank may purchase additional licences (maximum 1,00,000) at the same rate as discovered in the RFP during the Contract Validity of 05 years.

***** This will be the Total Cost of Ownership (TCO)/Total Project Cost and should be quoted in the reverse auction.

Breakup of Taxes and Duties

Sr. No.	Name of activity/Services	Tax 1	Tax 2	Tax 3
		Mention Name of Tax		
		GST%		
1.				
2.				
3.				
Grand Total				

Name & Signature of authorized signatory
Seal of Company
Illustration

Particulars	Indicative Price Bid Quote (INR)	Proportion to Total Cost 'G' (in %age) of indicative price bid	Final Price (INR) in reverse auction	Minimum final price should not be below (INR)	Maximum final price should not exceed (INR)
A	*B*	*C*	*D**	*E (95% of D)*	*F (95% of D)*
Item 1	25	13.16	9.87	9.38	10.36
Item 2	50	26.32	19.74	18.75	20.72
Item 3	75	39.47	29.60	28.13	31.09
Item 4	40	21.05	15.79	15.00	16.58
Grand Total (1 + 2 + 3 + 4) = G	**190**	**100**	**75**		

* Ideal final price breakup based on final price of INR 75 quoted in the reverse auction.

Appendix–G

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.>

Date:

To,

_____
_____
_____

Dear Sir,

Ref.: RFP No.: _____ Dated: _____

This is to certify that proposed _____ <details of services> is having the local content of _____ % as defined in the above-mentioned RFP.

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

Signature of Statutory Auditor/Cost Auditor
Registration Number:
Seal

Counter-signed:

Bidder **OEM**

< Certified copy of board resolution for appointment of statutory/cost auditor should also be enclosed with the certificate of local content.>

Appendix–H

BANK GUARANTEE FORMAT

(TO BE STAMPED AS AN AGREEMENT)

1. THIS BANK GUARANTEE AGREEMENT executed at _____this _____day of _____201 by _____ (Name of the Bank) _____ having its Registered Office at _____and its Branch at _____ (hereinafter referred to as "the Guarantor", which expression shall, unless it be repugnant to the subject, meaning or context thereof, be deemed to mean and include its successors and permitted assigns) IN FAVOUR OF State Bank of India, a Statutory Corporation constituted under the State Bank of India Act, 1955 having its Corporate Centre at State Bank Bhavan, Nariman Point, Mumbai and one of its offices at_____(procuring office address), hereinafter referred to as "SBI" which expression shall, unless repugnant to the subject, context or meaning thereof, be deemed to mean and include its successors and assigns).

2. WHEREAS M/s_____, incorporated under _____ Act having its registered office at _____ and principal place of business at _____ (hereinafter referred to as "Service Provider/ Vendor" which expression shall unless repugnant to the context or meaning thereof shall include its successor, executor & assigns) has agreed to develop, implement and support _____ (name of Service) (hereinafter referred to as "Services") to SBI in accordance with the Request for Proposal (RFP) No. **SBI/GITC/Platform Engineering-I/2021/2022/809 Dated: 06-Dec-2021**.

3. WHEREAS, SBI has agreed to avail the Services from Service Provider for a period of _____ year(s) subject to the terms and conditions mentioned in the RFP.

4. WHEREAS, in accordance with terms and conditions of the RFP/Purchase order/Agreement dated_____, Service Provider is required to furnish a Bank Guarantee for a sum of Rs._____/- (Rupees _____ only) for due performance of the obligations of Service Provider in providing the Services, in accordance with the RFP/Purchase order/Agreement guaranteeing payment of the said amount of Rs._____/- (Rupees _____ only) to SBI, if Service Provider fails to fulfill its obligations as agreed in RFP/Agreement.

5. WHEREAS, the Bank Guarantee is required to be valid for a total period of _____ months and in the event of failure, on the part of Service Provider, to fulfill any of its

commitments / obligations under the RFP/Agreement, SBI shall be entitled to invoke the Guarantee.

AND WHEREAS, the Guarantor, at the request of Service Provider, agreed to issue, on behalf of Service Provider, Guarantee as above, for an amount of Rs._____/- (Rupees _____ only).

NOW THIS GUARANTEE WITNESSETH THAT

1. In consideration of SBI having agreed to entrust Service Provider for rendering Services as mentioned in the RFP, we, the Guarantors, hereby unconditionally and irrevocably guarantee that Service Provider shall fulfill its commitments and obligations in respect of providing the Services as mentioned in the RFP/Agreement and in the event of Service Provider failing to perform / fulfill its commitments / obligations in respect of providing Services as mentioned in the RFP/Agreement, we (the Guarantor) shall on demand(s), from time to time from SBI, without protest or demur or without reference to Service Provider and not withstanding any contestation or existence of any dispute whatsoever between Service Provider and SBI, pay SBI forthwith the sums so demanded by SBI not exceeding Rs._____/- (Rupees _____only).

2. Any notice / communication / demand from SBI to the effect that Service Provider has failed to fulfill its commitments / obligations in respect of rendering the Services as mentioned in the Agreement, shall be conclusive, final & binding on the Guarantor and shall not be questioned by the Guarantor in or outside the court, tribunal, authority or arbitration as the case may be and all such demands shall be honoured by the Guarantor without any delay.

3. We (the Guarantor) confirm that our obligation to the SBI, under this Guarantee shall be independent of the agreement or other understandings, whatsoever, between the SBI and Service Provider.

4. This Guarantee shall not be revoked by us (the Guarantor) without prior consent in writing of the SBI.

WE (THE GUARANTOR) HEREBY FURTHER AGREE & DECLARE THAT-

i. Any neglect or forbearance on the part of SBI to Service Provider or any indulgence of any kind shown by SBI to Service Provider or any change in the terms and conditions of the Agreement or the Services shall not, in any way, release or discharge the Bank from its liabilities under this Guarantee.

ii. This Guarantee herein contained shall be distinct and independent and shall be enforceable against the Guarantor, notwithstanding any Guarantee or Security now or hereinafter held by SBI at its discretion.

iii. This Guarantee shall not be affected by any infirmity or absence or irregularity in the execution of this Guarantee by and / or on behalf of the Guarantor or by merger or amalgamation or any change in the Constitution or name of the Guarantor.

iv. The Guarantee shall not be affected by any change in the constitution of SBI or Service Provider or winding up / liquidation of Service Provider, whether voluntary or otherwise

v. This Guarantee shall be a continuing guarantee during its validity period.

vi. This Guarantee shall remain in full force and effect for a period of __ year(s) _____ month(s) from the date of the issuance i.e. up to _____. Unless a claim under this Guarantee is made against us on or before _____ , all your rights under this Guarantee shall be forfeited and we shall be relieved and discharged from all liabilities there under.

vii. This Guarantee shall be governed by Indian Laws and the Courts in Mumbai, India alone shall have the jurisdiction to try & entertain any dispute arising out of this Guarantee.

Notwithstanding anything contained herein above:

i. Our liability under this Bank Guarantee shall not exceed Rs_____/- (Rs. _____only)

ii. This Bank Guarantee shall be valid upto_____

iii. We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if SBI serve upon us a written claim or demand on or before _____

Yours faithfully,

For and on behalf of bank.

_____

Authorised official

Appendix–I

PENALTIES

Bidder has to ensure the Solution/support should comply the RFP/SLA terms and penalties will be imposed on breach of RFP/SLA terms as mentioned below.

PENALTY FOR NON-PERFORMANCE OF SLA

Severity	***Description***	***Response Time***	***Resolution Time***	***Penalty***
Critical	Operations Stopped. i.e. (ESS full infrastructure non-functional OR Bank's business critical application servers like CBS, INB, Yono and other Financial transaction related application completely stop due to ESS agent or new signature/pattern deployed or non-functioning of ESS agent due to its engine updates).	01 Hours	04 Hours	Rs. 25,000/- per Hrs after resolution time limit crossed
High	Operations Restricted/Impacted partially. i.e. (ESS infrastructure partially non-functional OR Bank's business critical application servers like CBS, INB, Yono and other Financial transaction related application partially stop/ i.e. some services are impacting due to ESS agent or new signature/pattern deployed or non-functioning of ESS agent due to its engine updates).	03 Hours	08 Hours	Rs. 15,000/- per Hrs after resolution time limit crossed
Medium	Operations completely Stopped for Non- Financial application. i.e. (Bank's non-critical application servers completely stop i.e. services are stopped due to ESS agent or new signature/pattern deployed or	05 Hours	12 Hours	Rs. 10,000/- per Hrs after resolution time limit crossed

	non-functioning of ESS agent due to its engine updates).			
Low/Minor	Operations partially Stopped for Non- Financial application. i.e. (Bank's non-critical application servers partially stop i.e. some services are impacted due to ESS agent or new signature/pattern deployed or non-functioning of ESS agent due to its engine updates).	08 Hours	24 Hours	Rs. 5,000/- per Hrs after resolution time limit crossed

Service Level Category	SLA Measure	Penalty Calculation
Application Uptime/Downtime/ RTO	*Application Uptime >99%,*	Rs 2000 Per Hours of delay.
Successful bidder has to submit the project implementation plan, architecture diagram (HLD & LLD), and hardware requirements (for on-premises components).	01 week of issuance of Purchase Order	Rs 1000 Per Day for delay.
Installation and configuration of the solution for UAT set up.	06 weeks of issuance of Purchase Order	Rs 1000 Per Day for delay.
UAT clearance and Security Review of the solution and closure of observations of security review and readiness for production setup. Helpdesk setup and manpower deployment	14 weeks of issuance of Purchase Order	Rs 1000 Per Day for delay.
Production roll-out (Pilot)	16 weeks of issuance of Purchase Order	Rs 1000 Per Day for delay.
Periodical training	The OEM/SI should provide product free training 04 times to at	Rs 500 Per Day for delay after breach of SLA Measure. The Solution

	least **10** SBI officials each year and designated officials at OEM's R&D center.	delivery timelines in Scope of Work Appendix-E
Reports	*Delay of more than 01 Days from the requirement raised by the Bank*	Rs 500 Per Day for delay after breach of SLA Measure. The Solution delivery timelines in Scope of Work Appendix-E

PENALTY TABLE- A –

Endpoint security solution signature/pattern/updates

System Integrator will ensure that the servers/ desktops and endpoints have updated signatures based on the different levels mentioned below.

Level 0- 99.99 % of all Endpoint security solution infrastructure servers/Data Center Servers/other critical servers in domestic or FO locations.
Level-1: 99.0 % at Branch servers.
Level-2: 97.0 % at all desktops/ nodes/ endpoints including customer touch point.
Level-3: 96.0 % at all roaming endpoints and endpoints on VSAT branches.

Level	Particulars	Agreed SLA %	In case of breach of SLA, Penalty to be recovered from SI,
Level-0	All online servers except Branch Servers	99.99 %	99.01% - <99.99% Rs. 20000/- per month or part thereof <99% Rs. 50,000/- per month or part thereof
Level-1	All online Branch Servers/FO servers/other servers in LHO or admin offices if any	99.0 %	98.5%-<99.0% Rs.10,000/- /- per month or part thereof 98%-<98.5% Rs. 15,000/-/- per month or part thereof <98% Rs. 25000/- per month or part thereof
Level-2	All online desktops / nodes/endpoints including branch customer touch points	97.0 %	96%-<97% Rs.5,000/-- per month or part thereof 95%-<96% Rs. 15,000/- per month or part thereof 94%-<95% Rs. 30,000/- per month or part thereof

			<94% Rs. 50,000/- per month or part thereof
Level-3	All online roaming endpoints and endpoints on VSAT branches	96.0 %	94%-<96% Rs.5,000/- per month or part thereof 92%-<94% Rs. 15,000/- per month or part thereof 93%-<94% Rs. 30,000/- per month or part thereof <93% Rs. 50,000/- per month or part thereof

PENALTY TABLE-B:

SI will be primarily responsible for identification, detection and remediation of Fixing Zero Day Viruses/Un-identified Threats in coordination with OEM. Any delay will be dealt as per this penalty clause.

Hours	Penalty
Up to 4 Hrs.	No penalty
Between 4 Hour to 8 Hrs.	Rs.3000/- per hour of delay per case
Between 8 hrs. to 12 hrs.	Rs.5000/- per hour of delay per case
Between 12 hrs. to 24 hrs.	Rs.10000/- per hour of delay per case
Between 24 hrs. to 48 hrs.	Rs.15000/- per hour of delay per case
Above 48 hrs.	Rs.20000/- per hour of delay per case

PENALTY FOR NON-PERFORMANCE AT HELP DESK:

Service Area	SLA measurement	Penalty of 10% on Monthly Support Services bill, Maximum 10% on Yearly bill		Calculate penalty on
		99.9 %	1% for every 1% shortfall from the stipulated service level	

Help Desk	Time taken for resolution of calls (99.9% of the calls should be resolved within the stipulated response time)	More than or equal to 99.9 % of service level	Less than 99.9 % of service level	*10% Penalty will be deducted on Yearly support Services Payment after breach of SLA*

PENALTY FOR INCIDENTS OR APPLICATION DOWNTIME:
Definitions of category of incident:

Category of incident	**Service Area**
Low/Minor	Resolution of Endpoints issue related with Endpoint security solution (No major impact on Endpoint functionality)
Medium	Non-Isolation/Quarantine/blocking/killing of malicious file, files malware, process, behaviour, and isolation of Endpoint from Network
High/Major	Not Fixing Zero Day Malware/Un-identified Threats, IOCs
Critical	Operation Down, Compromise of Banks Endpoints, loaded with Endpoint security solution
False Positive	Reporting of false positive which impacted the operation major, critical.

Severity	**Hours**	**Penalty**
Priority-1 (Critical)	Up to 1 Hrs.	No penalty
	Between 1 Hour to 2 Hrs.	Rs.2000/- per hour of delay per case
	Between 2 Hrs. to 4 Hrs.	Rs.5000/- per hour of delay per case
	Between 4 hrs. to 6 Hrs.	Rs.10000/- per hour of delay per case
	Between 6 hrs. to 8 Hrs.	Rs.15000/- per hour of delay per case
	Between 8 hrs. to 10 Hrs.	Rs.20000/- per hour of delay per case

	Above 10 Hrs.	Rs.25000/- per hour of delay per case

Severity	Hours	Penalty
Priority-2 (High/Major)	Up to 4 Hrs.	No penalty
	Between 4 hrs. to 6 Hrs.	Rs.2000/- per hour of delay per case
	Between 6 hrs. to 8 Hrs.	Rs.3000/- per hour of delay per case
	Between 8 hrs. to 10 Hrs.	Rs.5000/- per hour of delay per case
	Above 10 Hrs.	Rs.10000/- per hour of delay per case

Severity	Hours	Penalty
Priority-3 (Medium)	Up to 12 Hrs.	No penalty
	Between 12 Hour to 24Hrs.	Rs.1000/- per hour of delay per case
	Between 24 Hrs. to 48 Hrs.	Rs.5000/- per hour of delay per case
	Above 48 Hrs.	Rs.8000/- per hour of delay per case

Severity	Hours	Penalty
Priority-4 (Low/Minor)	Up to 24 Hrs.	No penalty
	Between 24 Hour to 48Hrs.	Rs.1000/- per hour of delay per case
	Above 48 Hrs.	Rs.2000/- per hour of delay per case

Severity	Hours
False Positive and any application impacted	*Penalty will be imposed as per above priorities level P1, P2, P3 and P4 depends upon the criticality of impacted application*

Penalties for Non-closure of ISD/SOC/IEHRT /IS Audit / CERTIN/ CERTINRBI Advisory/Alerts Vulnerability report shared in Endpoint security solution infrastructure and any other Audit Observations and non-availability of signature/remediation for new malwares.

Description	Months	Penalty
Vulnerability Closure	Report is shared by the Bank. All VA pertains to Endpoint security solution infrastructure must be closed within 01 months from date of report shared.	No penalty
	After 01 months from the date of report shared by Bank.	*Rs. 5000 per month*
Audit Observations Closure	Up to 01 Months	*No penalty*
	01 Month's to 03 Month's	*Rs. 100 per open observation.*
	03 Month's to 06 Month's	*Rs. 500 per open observation*
	06 Month's to 09 Month's	*Rs 1000 per open observation*
	After 09 Month's	*Rs. 2 Lac + Rs 10000 per open observations*
Non-availability of signature for remediation of the malware and IT-Threats	Under any circumstances equal to or more than 03 instances of per month of the signature / remediation not being made available to the Bank.	5% of monthly invoice value.
	Second time repetition of the similar instances of signature / remediation not being made available to the Bank.	Bank may invoke limitation of liability mentioned in para no 31 of this RFP
	Global Signature not being made available to Bank more than 06 Hrs. from their release by other OEM of ESS /EPP/AV OEM's.	5% of monthly invoice value.
	Second time repetition instance of the Signature not being made available to Bank more than 06 Hrs. from their release by other	Bank may invoke limitation of liability mentioned in para no 31 of this RFP

	OEM of ESS /EPP/AV OEM's.	

Non-Availability of Helpdesk Team Members (L1, L2, L3 Team lead and MIS Manager).

In case any of the TEAM member including Team lead, MIS manager, L3, L2 and L1 leaving the project or SI switching the resources in any other project from SBI should inform Bank in written and have to server 3-month notice. During the notice period SI has to arrange the new resource within 2 month and 1 month of knowledge transfer to new resource. The resource who is leaving/switching the project will not be allowed to join SBI Bank other departments project for next one year. On boarding date of the resources in SBI will be considered as date after 10 days from submission of documents required for permanent access card creation in SBI. In case SI fails in managing the resources on time then Bank will impose the penalty as mention below

Support Team Member	Days	Penalty
Non-Availability of Team Lead	Resource has to server notice period of 03 month before leaving the project.	Twice of the gross monthly salary plus Rs. 5000/- per day after end of notice period
Non-Availability of L3	Resource has to server notice period of 03 month before leaving the project.	Thrice of the gross monthly salary plus Rs. 10000/- per day after end of notice period
Non-Availability of L2	Resource has to server notice period of 03 month before leaving the project.	Twice of the gross monthly salary plus Rs. 5000/- per day after end of notice period
Non-Availability of L1	Resource has to server notice period of 03 month before leaving the project.	Twice of the gross monthly salary plus Rs. 4000/- per day after end of notice period
Non-Availability of MIS Manager	Resource has to server notice period of 03 month before leaving the project.	Twice of the gross monthly salary plus Rs. 3000/- per day after end of notice period
Any of the above mention resources left the project on urgency	Without serving 03 months' notice period.	Thrice of the gross monthly salary of resources leaving the project or bidders plus Rs. 25000/-

Penalty for non-compliance of deployment schedule

Endpoint security solution Deployment Schedule on endpoints:

The date intimation for rollout of the Endpoint Security Solution to the SI will be confirmed by the Bank for Project Schedule after ISD clearance.

Sr. No.	Endpoints Description	First month of successful pilot out	Second month of successful pilot out	Penalty
1	Desktop 2.65 lac	40%	60%	5% invoice value submitted by SI to bank for payment.
2	Virtual Servers 68,000	30%	70%	5% invoice value submitted by SI to bank for payment.
3	Physical Servers (Windows & Non-Windows) 15000	30%	70%	5% invoice value submitted by SI to bank for payment.
4.	Banks Private cloud 15000	30%	70%	5% invoice value submitted by SI to bank for payment.
5.	Roaming endpoints i.e. VPN Laptops, Bank Laptops iPad, Mobile (50,000)	40%	60%	5% invoice value submitted by SI to bank for payment.

Penalty for non-compliance of above mention deployment schedule on endpoints:

A penalty will be imposed on the selected service integrator (SI) in case of delay and non-compliance of above deployment schedule for new endpoint security solution for remaining percentage of deployment in month from the invoice submitted to Bank for payment. The overall delay in implementation of project will be calculated milestone wise.

Appendix–J

SERVICE LEVEL AGREEMENT

Agreement for
Procurement, implementation, integration, maintenance, administration, onsite support and licenses for centralized Endpoint Protection Platform (EPP), Application Change Control (ACC), File Integrity Monitoring (FIM) and Early Detection and Response (EDR) as a comprehensive Endpoint Security Solution (ESS) for State Bank Group

BETWEEN

STATE BANK OF INDIA,
Deputy General Manager
IT-Platform Engineering-I Department,
State bank of India Global IT Centre,
Ground Floor 'A'- Wing, Plot no 8/9/10,
Sector -11, CBD Belapur
Navi Mumbai- 400614 [1]

AND

_____ [2]

Date of Commencement : _____ [3]
Date of Expiry :_____

1 Office/ Department/ Branch which is executing the Agreement or the nodal department in the matter.
2 The other Party (Contractor/ Service Provider) to the Agreement
3 Effective Date from which the Agreement will be operative.

Table of Contents for SLA

Sl. No.	Items
1	DEFINITIONS & INTERPRETATION
2	SCOPE OF WORK
3	FEES /COMPENSATION
4	LIABILITIES/OBLIGATION
5	REPRESENTATIONS &WARRANTIES
6	GENERAL INDEMNITY
7	CONTINGENCY PLANS
8	TRANSITION REQUIREMENT
9	LIQUIDATED DAMAGES
10	RELATIONSHIP BETWEEN THE PARTIES
11	SUB CONTRACTING
12	INTELLECTUAL PROPERTY RIGHTS
13	INSPECTION AND AUDIT
14	CONFIDENTIALITY
15	TERMINATION
16	DISPUTE REDRESSAL MACHANISM & GOVERNING LAW
17	WAIVER OF RIGHTS
18	LIMITATION OF LIABILITY
19	FORCE MAJEURE
20	NOTICES
21	GENERAL TERMS & CONDITIONS
22	ANNEXURE-A
23	ANNEXURE-B
24	ANNEXURE-C
25	ANNEXURE-D
26	ANNEXURE-E
27	ANNEXURE-F

This agreement ("Agreement") is made at_____ (Place) on this _____day of _____ 20__.

BETWEEN

State Bank of India, constituted under the State Bank of India Act, 1955 having its Corporate Centre at State Bank Bhavan, Madame Cama Road, Nariman Point, Mumbai-21 and its Global IT Centre at Sector-11, CBD Belapur, Navi Mumbai- 400614 through its Deputy General Manager, IT-Platform Engineering-I Department, State Bank of India Global IT Centre, Gr Floor 'A'- Wing, Plot no 8/9/10,Sector -11, CBD Belapur Navi Mumbai- 400614 [4] hereinafter referred to as "**the Bank**" which expression shall, unless it be repugnant to the context or meaning thereof, be deemed to mean and include its successors in title and assigns of First Part:

AND

_____[5] a private/public limited company/LLP/Firm <strike off whichever is not applicable> incorporated under the provisions of the Companies Act, 1956/ Limited Liability Partnership Act 2008/ Indian Partnership Act 1932 <strike off whichever is not applicable>, having its registered office at _____ hereinafter referred to as "**Service Provider/ Vendor**", which expression shall mean to include its successors in title and permitted assigns of the Second Part:

WHEREAS The Bank" is carrying on business in Banking in India and overseas and desirous to avail services for Procurement, Implementation, Integration, Maintenance, Administration, Onsite Support and Licenses for Centralized Endpoint Protection Platform (EPP), Application Change Control (ACC), File Integrity Monitoring (FIM) and Early Detection and Response (EDR) as a comprehensive Endpoint Security Solution for State Bank Group;6

State Bank Group;7

(i) _____;

(ii) _____; and

[4]Name & Complete Address of the Dept.

5Name & Complete Address (REGISTERED OFFICE) of service Provider,

6 Please provide the brief introduction, facts and circumstances which lead to the present agreement (preamble of the agreement).

7 Please provide the brief introduction, facts and circumstances which lead to the present agreement (preamble of the agreement).

(iii) Service Provider is in the business of providing _____ and has agreed to provide the services as may be required by the Bank mentioned in the Request of Proposal (RFP) No. _____ dated _____issued by the Bank along with its clarifications/ corrigenda, referred hereinafter as a "RFP" and same shall be part of this Agreement.

NOW THEREFORE, in consideration of the mutual covenants, undertakings and conditions set forth below, and for other valid consideration the acceptability and sufficiency of which are hereby acknowledged, the Parties hereby agree to the following terms and conditions hereinafter contained:-

1. DEFINITIONS & INTERPRETATION

1.1 Definition

Certain terms used in this Agreement are defined hereunder. Other terms used in this Agreement are defined where they are used and have the meanings there indicated. Unless otherwise specifically defined, those terms, acronyms and phrases in this Agreement that are utilized in the information technology services industry or other pertinent business context shall be interpreted in accordance with their generally understood meaning in such industry or business context, unless the context otherwise requires/mentions, the following definitions shall apply:

1.1.1 'The Bank' shall mean the State Bank of India (including domestic branches and foreign offices), Subsidiaries and Joint Ventures, where the Bank has ownership of more than 50% of voting securities or the power to direct the management and policies of such Subsidiaries and Joint Ventures:< Strike of whichever is inapplicable.>

1.1.2 "Confidential Information" shall have the meaning set forth in Clause 14.

1.1.3 "Deficiencies" shall mean defects arising from non-conformity with the mutually agreed specifications and/or failure or non-conformity in the Scope of the Services.

1.1.4 "Documentation" will describe in detail and in a completely self-contained manner how the User may access and use the Endpoint Security Solution

<Strike off whichever is inapplicable>,[8] such that any reader of the Documentation can access, use and maintain all of the functionalities of the Endpoint Security Solution (Service)[9], without the need for any further instructions. 'Documentation' includes, user manuals, installation manuals, operation manuals, design documents, process documents, technical manuals, functional specification, software requirement specification, on-line tutorials/CBTs, system configuration documents, system/database administrative documents, debugging/diagnostics documents, test procedures, Review Records/ Test Bug Reports/ Root Cause Analysis Report, list of all Product components, list of all dependent/external modules and list of all documents relating to traceability of the Product as and when applicable etc.

1.1.5 "Intellectual Property Rights" shall mean, on a worldwide basis, any and all: (a) rights associated with works of authorship, including copyrights &moral rights; (b) Trade Marks; (c) trade secret rights; (d) patents, designs, algorithms and other industrial property rights; (e) other intellectual and industrial property rights of every kind and nature, however designated, whether arising by operation of law, contract, license or otherwise; and (f) registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

1.1.6 "Project Cost" means the price payable to Service Provider over the entire period of Agreement (i.e. Rs._____<in words>) for the full and proper performance of its contractual obligations.

1.1.7 "Request for Proposal (RFP)" shall mean RFP NO. _____ dated _____ along with its clarifications/ corrigenda issued by the Bank time to time.

1.1.8 "Root Cause Analysis Report" shall mean a report addressing a problem or non-conformance, in order to get to the 'root cause' of the problem, which thereby assists in correcting or eliminating the cause, and prevent the problem from recurring.

[8] Name of services
[9] Name of services

1.1.9 'Services' shall mean and include the Services offered by Service Provider under this Agreement more particularly described in Clause 2 of this Agreement.

1.2 **Interpretations:**

1.2.1 Reference to a person includes any individual, firm, body corporate, association (whether incorporated or not) and authority or agency (whether government, semi government or local).

1.2.2 The singular includes the plural and vice versa.

1.2.3 Reference to any gender includes each other gender.

1.2.4 The provisions of the contents table, headings, clause numbers, italics, bold print and underlining is for ease of reference only and shall not affect the interpretation of this Agreement.

1.2.5 The Schedules, Annexures and Appendices to this Agreement shall form part of this Agreement.

1.2.6 A reference to any documents or agreements (and, where applicable, any of their respective provisions) means those documents or agreements as amended, supplemented or replaced from time to time provided they are amended, supplemented or replaced in the manner envisaged in the relevant documents or agreements.

1.2.7 A reference to any statute, regulation, rule or other legislative provision includes any amendment to the statutory modification or re-enactment or, legislative provisions substituted for, and any statutory instrument issued under that statute, regulation, rule or other legislative provision.

1.2.8 Any agreement, notice, consent, approval, disclosure or communication under or pursuant to this Agreement is to be in writing.

1.2.9 The terms not defined in this agreement shall be given the same meaning as given to them in the RFP. If no such meaning is given technical words shall be understood in technical sense in accordance with the industrial practices.

1.3 **Commencement, Term & Change in Terms**

1.3.1 This Agreement shall commence from its date of execution mentioned above/ be deemed to have commenced from _____ (Effective Date).

1.3.2 This Agreement shall be in force for a period of _____ year(s) from Effective Date, unless terminated by the Bank by notice in writing in accordance with the termination clauses of this Agreement.

1.3.3 The Bank shall have the right at its discretion to renew this Agreement in writing, for a further term of _____ years on the mutually agreed terms & conditions.

2. SCOPE OF WORK

2.1 The scope and nature of the work which Service Provider has to provide to the Bank (Services) is described in **Annexure-A.**

2.2 The Bank may, at its sole discretion, provide remote access to its information technology system to IT Service Provider through secured Virtual Private Network (VPN) in order to facilitate the performance of IT Services. Such remote access to the Bank's information technology system shall be subject to the following:

2.1.1 Service Provider shall ensure that the remote access to the Bank's VPN is performed through a laptop/desktop ("Device") specially allotted for that purpose by the Service Provider and not through any other private or public Device.

2.1.2 Service Provider shall ensure that only its authorized employees/representatives access the Device.

2.1.3 Service Provider shall be required to get the Device hardened/configured as per the Bank's prevailing standards and policy.

2.1.4 Service Provider and/or its employee/representative shall be required to furnish an undertaking and/or information security declaration on the Bank's prescribed format before such remote access is provided by the Bank.

2.1.5 Service Provider shall ensure that services are performed in a physically protected and secure environment which ensures confidentiality and integrity of the Bank's data and artefacts, including but not limited to information (on customer, account, transactions, users, usage, staff, etc.), architecture (information, data, network, application, security, etc.), programming codes, access configurations, parameter settings, executable files, etc., which the Bank representative may inspect. Service Provider shall

facilitate and/ or handover the Device to the Bank or its authorized representative for investigation and/or forensic audit.

2.1.6 Service Provider shall be responsible for protecting its network and subnetworks, from which remote access to the Bank's network is performed, effectively against unauthorized access, malware, malicious code and other threats in order to ensure the Bank's information technology system is not compromised in the course of using remote access facility.

3. FEES /COMPENSATION

3.1 Professional fees

3.1.1 Service Provider shall be paid fees and charges in the manner detailed in here under, the same shall be subject to deduction of income tax thereon wherever required under the provisions of the Income Tax Act by the Bank. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by the Bank as per the laws and regulations for the time being in force. Nothing in the Agreement shall relieve Service Provider from his responsibility to pay any tax that may be levied in India on income and profits made by Service Provider in respect of this Agreement.

3.1.2 _____

3.1.3 _____

3.2 All duties and taxes (excluding[10] _____ or any other tax imposed by the Government in lieu of same), if any, which may be levied, shall be borne by Service Provider and Bank shall not be liable for the same. All expenses, stamp duty and other charges/ expenses in connection with execution of this Agreement shall be borne by Service Provider. _____ <insert tax payable by the Bank> or any other tax imposed by the Government in lieu of same shall be borne by the Bank on actual upon production of original receipt wherever required.

3.3 Service Provider shall provide a clear description quantifying the service element and goods element in the invoices generated by them.

[10] Please determine the applicability of the taxes.

3.4 **Payments**

3.4.1 The Bank will pay properly submitted valid invoices within reasonable period but not exceeding 30 (thirty) days after its receipt thereof. All payments shall be made in Indian Rupees.

3.4.2 The Bank may withhold payment of any product/services that it disputes in good faith, and may set-off penalty amount or any other amount which Service Provider owes to the Bank against amount payable to Service provider under this Agreement. However, before levying penalty or recovery of any damages, the Bank shall provide a written notice to Service Provider indicating the reasons for such penalty or recovery of damages. Service Provider shall have the liberty to present its case in writing together with documentary evidences, if any, within 21 (twenty one) days. Penalty or damages, if any, recoverable from Service Provider shall be recovered by the Bank through a credit note or revised invoices. In case Service Provider fails to issue credit note/ revised invoice, the Bank shall have right to withhold the payment or set-off penal amount from current invoices.

3.5 **Bank Guarantee and Penalties**

3.5.1 Service Provider shall furnish performance security in the form of Bank Guarantee for an amount of Rs. _____ valid for a period of _____year(s) ____month(s) from a Scheduled Commercial Bank other than State Bank of India in a format provided/ approved by the Bank.

3.5.2 The Bank Guarantee is required to protect the interest of the Bank against the risk of non-performance of Service Provider in respect of successful implementation of the project and/or failing to perform / fulfil its commitments / obligations in respect of providing Services as mentioned in this Agreement; or breach of any terms and conditions of the Agreement, which may warrant invoking of Bank Guarantee.

3.5.3 If at any time during performance of the contract, Service Provider shall encounter unexpected conditions impeding timely completion of the Services under the Agreement and performance of the services, Service Provider shall promptly notify the Bank in writing of the fact of the delay, it's likely duration and its cause(s). As soon as practicable, after receipt of

Service Provider's notice, the Bank shall evaluate the situation and may at its discretion extend Service Provider's time for performance, in which case the extension shall be ratified by the Parties by amendment of the Agreement.

3.5.4 Performance of the obligations under the Agreement shall be made by Service Provider in accordance with the time schedule[11] specified in this Agreement.

3.5.5 Service Provider shall be liable to pay penalty at the rate mentioned in **Annexure-E** in respect of any delay beyond the permitted period in providing the Services.

3.5.6 No penalty shall be levied in case of delay(s) in deliverables or performance of the contract for the reasons solely and directly attributable to the Bank. On reaching the maximum of penalties specified the Bank reserves the right to terminate the contract.

4. LIABILITIES/OBLIGATION

4.1 **The Bank's Duties /Responsibility(if any)**

(i) Processing and authorising invoices

(ii) _____

4.2 **Service Provider Duties**

(i) Service Delivery responsibilities

(a) To adhere to the service levels documented in this Agreement.

(b) Service Provider shall ensure that Service Provider's personnel and its sub-contractors (if allowed) will abide by all reasonable directives issued by the Bank, including those set forth in the Bank's then-current standards, policies and procedures (to the extent applicable), all on-site rules of behaviour, work schedules, security procedures and other standards, policies and procedures as established by the Bank from time to time.

(c) Service Provider agrees and declares that it shall be the sole responsibility of Service Provider to comply with the provisions of all the applicable

[11] Please ensure that the time scheduled is suitably incorporated in the Agreement.

laws for the time being in force including but not limited to Information Technology Act, 2000 and rules thereof concerning or in relation to rendering of Services by Service Provider as envisaged under this Agreement.

(ii) Security Responsibility

(a) Service Provider shall maintain the confidentiality of the Bank's resources and other intellectual property rights.

(b) Service Provider shall implement and maintain reasonable security practices and procedures as defined under Section 43A of Information Technology Act, 2000 and rules thereof.

(c) Without the Bank's prior written permission, Service Provider shall not store or share Bank's materials including Confidential Information outside the geographical boundary of India or in/with a public cloud.

(d) Service Provider shall ensure that its environment is suitably protected from external threats by way of firewall.

(e) Service Provider shall follow the best practices of creation of separate network zones (VLAN Segments) for Web, App, DB and different zones for critical applications, non-critical applications, UAT etc.

(f) Service Provider shall take action immediately to identify and mitigate an information security incident and to carry out any recovery or remedies. Service Provider shall first obtain the Bank's approval of the content of any filing, communications, notices, press release or reports related to any security breach prior to any publication or communication thereof to any third party. Service Provide shall maintain a well understood reporting procedure for security incidents and a copy of such procedure shall be made available to the Bank.

5. REPRESENTATIONS &WARRANTIES

5.1 Each of the Parties represents and warrants in relation to itself to the other that:

5.1.1 It has all requisite corporate power and authority to execute, deliver and perform its obligations under this Agreement and has been fully authorized through applicable corporate process to do so.

5.1.2 The person(s) signing this Agreement on behalf of the Parties have the necessary authority and approval for execution of this document and to bind his/their respective organization for due performance as set out in this Agreement. It has all necessary statutory and regulatory permissions, approvals and permits for the running and operation of its business.

5.1.3 It has full right, title and interest in and to all software, copyrights, trade names, trademarks, service marks, logos symbols and other proprietary marks (collectively 'IPR') (including appropriate limited right of use of those owned by any of its vendors, affiliates or subcontractors) which it provides to the other Party, for use related to the Services to be provided under this Agreement.

5.1.4 It will provide such cooperation as the other Party reasonably requests in order to give full effect to the provisions of this Agreement.

5.1.5 The execution and performance of this Agreement by either of the Parties does not and shall not violate any provision of any of the existing Agreement with any of the party and any other third party.

5.2 **Additional Representation and Warranties by Service Provider**

5.2.1 Service Provider shall perform the Services and carry out its obligations under the Agreement with due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used in the industry and with professional standards recognized by international professional bodies and shall observe sound management practices. It shall employ appropriate advanced technology and safe and effective equipment, machinery, material and methods.

5.2.2 Service Provider has the requisite technical and other competence, sufficient, suitable, qualified and experienced manpower/personnel and expertise in providing the Services to the Bank.

5.2.3 Service Provider shall duly intimate to the Bank immediately, the changes, if any in the constitution of Service Provider.

5.2.4 Service Provider warrants that to the best of its knowledge, as on the Effective Date of this Agreement, the Services provided by Service

Provider to the Bank do not violate or infringe any patent, copyright, trademarks, trade secrets or other intellectual property rights of any third party.

5.2.5 Service provider shall ensure that all persons, employees, workers and other individuals engaged by or sub-contracted (if allowed) by Service Provider in rendering the Services under this Agreement have undergone proper background check, police verification and other necessary due diligence checks to examine their antecedence and ensure their suitability for such engagement. No person shall be engaged by Service provider unless such person is found to be suitable in such verification and Service Provider shall retain the records of such verification and shall produce the same to the Bank as and when requested.

5.2.6 Service Provider warrants that the software deployed/ upgraded for providing Services as a part of this Agreement is free from malware, free from any obvious bugs, and free from any covert channels in the code (of the versions of the applications/software being deployed as well as any subsequent versions/modifications done). Software deployed/ upgraded for providing Services as a part of this Agreement shall remain free from OWASP Top 10 vulnerabilities (latest) during the term of this Agreement.

5.2.7 Service Provider represents and warrants that its personnel shall be present at the Bank premises or any other place as the bank may direct, only for the Services and follow all the instructions provided by the Bank; act diligently, professionally and shall maintain the decorum and environment of the Bank; comply with all occupational, health or safety policies of the Bank.

5.2.8 Service Provider warrants that it shall be solely liable and responsible for compliance of applicable Labour Laws in respect of its employee, agents, representatives and sub-contractors (if allowed) and in particular laws relating to terminal benefits such as pension, gratuity, provided fund, bonus or other benefits to which they may be entitled and the laws relating to contract labour, minimum wages, etc., and the Bank shall have no liability in this regard.

5.2.9 Service Provider agrees that the Bank either itself or through its authorized representative shall have right to perform ethical hacking on public IPs and URLs of Service Provider, wherein the Bank has integrations.

5.2.10 Service Provider agrees that it shall communicate to the Bank well in advance along with detail plan of action, if any changes in Service Provider's environment/infrastructure is of the nature that may have direct or indirect impact on the Services provided under this Agreement or operations of its Services.

5.2.11 Service Provider at its own expenses, agrees to provide audit report of the process and infrastructure from CERT-In empanelled ISSP, periodically, at least once in a year or as requested by the Bank.

5.2.12 Service Provider shall ensure confidentiality, integrity and availability of the Bank's information at all times and shall comply with regard to the followings:

a) Acceptable Usage Policy: Information assets of Service Provider should be provided to its authorized users only for the intended purpose and users shall adhere to safe and acceptable usage practices.

b) Email Usage: The employees of Service Provider shall use authorized media only for email communication.

c) Password Management: Service Provider shall have a password management system in place, which ensures secure passwords.

d) Physical and Environmental Security: Service Provider shall provide sufficient guidance for its employees with respect to physical and environmental security.

e) Logical Access Control and User Access Management: The access to information and information systems shall be according to the principles of "least privilege" and "need to know" basis to authorized users of Service Provider.

f) Infrastructure Security: Service Provider shall ensure correct and secure operations of information processing facilities.

g) Change Management: Service Provider shall provide a managed and orderly method in which changes to the information technology

environment are requested, tested and approved prior to installation or implementation.

h) Information Security Incident Management: Service provider shall ensure effective management of information security incidents, including the preservation of digital evidence.

i) Communications Strategy: Service provider shall ensure prevention of unauthorized access to communications traffic, or to any written information that is transmitted or transferred.

j) Service Provider Relationship: Service provider shall ensure that information security risks related to outsourcing of Services to any other party, if permitted by the Bank, shall be assessed and managed regularly, to the satisfaction of the Bank.

k) Digital Risk: Service Provider shall ensure that electronic data is gathered and preserved in a systematic, standardized and legal manner to ensure the admissibility of the evidence for the purpose of any legal proceedings or investigations, whenever demanded by the Bank.

l) Change Management: Service Provider shall provide a managed and orderly method in which changes to the information technology environment (including, database, operating system, application, networking etc.) are requested, tested and approved prior to installation or implementation.

m) Port Management: Service Provider shall ensure that the controls are implemented for secure port management so as to protect the network from unauthorized access.

n) Patch Management: Service Provider shall ensure that the security patches to information assets and systems are correctly and completely updated in a timely manner for known vulnerabilities.

o) Backup Management: Service Provider shall ensure that regular backup is taken so that when necessary, information may be restored from backup media to return the application, database, operating system etc. to production status.

p) Access Management: Service Provider shall limit access to information and information processing facilities for authorized users only.

q) Log Management: Logging shall be enabled on all systems of Service Provider to ensure audit trail is maintained every time.

r) Service Provider shall have an anti-virus solution with regular updates to protect their system against malicious attacks in the form of virus, malware, trojans etc.

6. GENERAL INDEMNITY

6.1 Service Provider agrees and hereby keeps the Bank indemnified against all claims, actions, loss, damages,, costs, expenses, charges, including legal expenses (Attorney, Advocates fees included) which the Bank may suffer or incur on account of (i) Services Provider's breach of its warranties, covenants, responsibilities or obligations; or (ii) breach of confidentiality obligations mentioned in this Agreement; or (iii) any willful misconduct and gross negligent acts on the part of employees, agents, representatives or sub-contractors (if allowed) of Service Provider. Service Provider agrees to make good the loss suffered by the Bank.

6.2 Service Provider hereby undertakes the responsibility to take all possible measures, at no additional cost, to avoid or rectify any issues which thereby results in non-performance of Service Provider systems including deliverables within reasonable time. The Bank shall report as far as possible all material defects to Service Provider without undue delay. Service Provider also undertakes to co-operate with other service providers thereby ensuring expected performance covered under scope of work.

7. CONTINGENCY PLANS

7.1 Service Provider shall arrange and ensure proper data recovery mechanism, attrition plan and other contingency plans to meet any unexpected obstruction to the Service Provider or any employees or sub-contractors (if allowed) of Service Provider in rendering the Services or any part of the same under this Agreement to the Bank. Service Provider at Banks discretion shall co-operate with the Bank in case on any contingency.

7.2 Service Provider shall have defined business continuity management and disaster recovery procedures in place for effective handling of critical business

processes in situation of any incident disrupting the Services under this Agreement. Service Provider shall carry out periodic drill activity to ensure the effectiveness of business continuity management and disaster recovery procedures and reports of such activities shall be shared with the Bank.

8. TRANSITION REQUIREMENT

In the event of failure of Service Provider to render the Services or in the event of termination of Agreement or expiry of term or otherwise, without prejudice to any other right, the Bank at its sole discretion may make alternate arrangement for getting the Services contracted with another vendor. In such case, the Bank shall give prior notice to the existing Service Provider. The existing Service Provider shall continue to provide services as per the terms of the Agreement until a 'New Service Provider' completely takes over the work. During the transition phase, the existing Service Provider shall render all reasonable assistances to the new Service Provider within such period prescribed by the Bank, at no extra cost to the Bank, for ensuring smooth switch over and continuity of Services, provided where transition services are required by the Bank or New Service Provider beyond the term of this Agreement, reasons for which are not attributable to Service Provider, payment shall be made to Service Provider for such additional period on the same rates and payment terms as specified in this Agreement. If existing Service Provider is found to be in breach of this obligation, they shall be liable for paying a penalty of Rs._____ on demand to the Bank, which may be settled from the payment of invoices or bank guarantee for the contracted period. Transition & Knowledge Transfer plan is mentioned in Annexure F.

9. LIQUIDATED DAMAGES

If Service Provider fails to deliver and perform any or all the Services within the stipulated time, schedule as specified in this Agreement, the Bank may, without prejudice to its other remedies under the Agreement, and unless otherwise extension of time is agreed upon without the application of liquidated damages, deduct from the Project Cost, as liquidated damages a sum equivalent to ___% of total Project cost for delay of each week or part thereof maximum

up to ___% of total Project cost. Once the maximum deduction is reached, the Bank may consider termination of the Agreement.

10. RELATIONSHIP BETWEEN THE PARTIES

10.1 It is specifically agreed that Service Provider shall act as independent service provider and shall not be deemed to be the Agent of the Bank except in respect of the transactions/services which give rise to Principal - Agent relationship by express agreement between the Parties.

10.2 Neither Service Provider nor its employees, agents, representatives, Sub-Contractors shall hold out or represent as agents of the Bank.

10.3 None of the employees, representatives or agents of Service Provider shall be entitled to claim any absorption or any other claim or benefit against the Bank.

10.4 This Agreement shall not be construed as joint venture. Each Party shall be responsible for all its obligations towards its respective employees. No employee of any of the two Parties shall claim to be employee of other Party.

10.5 All the obligations towards the employee(s) of a Party on account of personal accidents while working in the premises of the other Party shall remain with the respective employer and not on the Party in whose premises the accident occurred unless such accidents occurred due to gross negligent act of the Party in whose premises the accident occurred.

10.6 For redressal of complaints of sexual harassment at workplace, Parties agree to comply with the policy framed by the Bank (including any amendment thereto) in pursuant to the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 including any amendment thereto.

11. SUB CONTRACTING

As per the scope of this Agreement **sub-contracting is not permitted**.

12. INTELLECTUAL PROPERTY RIGHTS

12.1 For any technology / software / product used by Service Provider for performing Services for the Bank as part of this Agreement, Service Provider shall have right to use as well as right to license such technology/ software / product. The Bank shall not be liable for any license or IPR violation on the part of Service Provider.

12.2 Without the Bank's prior written approval, Service provider will not, in performing the Services, use or incorporate link to or call or depend in any way upon, any software or other intellectual property that is subject to an Open Source or Copy left license or any other agreement that may give rise to any third-party claims or to limit the Bank's rights under this Agreement.

12.3 Subject to clause 12.4 and 12.5 of this Agreement, Service Provider shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the Bank against all costs, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from the Services or use of the technology / software / products or any part thereof in India or abroad.

12.4 The Bank will give (a) notice to Service Provider of any such claim without delay/provide reasonable assistance to Service Provider in disposing of the claim; (b) sole authority to defend and settle such claim and; (c) will at no time admit to any liability for or express any intent to settle the claim provided that (i) Service Provider shall not partially settle any such claim without the written consent of the Bank, unless such settlement releases the Bank fully from such claim, (ii) Service Provider shall promptly provide the Bank with copies of all pleadings or similar documents relating to any such claim, (iii) Service Provider shall consult with the Bank with respect to the defense and settlement of any such claim, and (iv) in any litigation to which the Bank is also a party, the Bank shall be entitled to be separately represented at its own expenses by counsel of its own selection.

12.5 Service Provider shall have no obligations with respect to any infringement claims to the extent that the infringement claim arises or results from: (i) Service Provider's compliance with the Bank's specific technical designs or instructions (except where Service Provider knew or should have known that such compliance was likely to result in an Infringement Claim and Service Provider did not inform the Bank of the same); or (ii) any unauthorized modification or alteration of the deliverable (if any) by the Bank.

13. INSPECTION AND AUDIT

13.1 It is agreed by and between the parties that Service Provider shall be subject to annual audit by internal/external Auditors appointed by the Bank/ inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ software) and Services etc. provided to the Bank and Service Provider shall submit such certification by such Auditors to the Bank. Service Provider and or his / their outsourced agents / sub – contractors (if allowed by the Bank) shall facilitate the same. The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by Service Provider. Service Provider shall, whenever required by such Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the Bank. Except for the audit done by Reserve Bank of India or any statutory/regulatory authority, the Bank shall provide reasonable notice not less than 7 (seven) days to Service Provider before such audit and same shall be conducted during normal business hours.

13.2 Where any Deficiency has been observed during audit of Service Provider on the risk parameters finalized by the Bank or in the certification submitted by the Auditors, it is agreed upon by Service Provider that it shall correct/ resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the Deficiencies. It is also agreed that Service Provider shall provide certification of the auditor to the Bank regarding compliance of the observations made by the auditors covering the respective risk parameters against which such Deficiencies observed.

13.3 Service Provider further agrees that whenever required by the Bank, it will furnish all relevant information, records/data to such auditors and/or inspecting officials of the Bank/ Reserve Bank of India and/or any regulatory authority(ies). The Bank reserves the right to call for and/or retain any relevant information / audit reports on financial and security reviews with their findings undertaken by Service Provider. However, Service Provider shall not be

obligated to provide records/ data not related to Services under the Agreement (e.g. internal cost breakup etc.).

14. CONFIDENTIALITY

14.1 "Confidential Information" mean all information which is material to the business operations of either party or its affiliated companies, designated as being confidential or which, under the circumstances surrounding disclosure out to be treated as confidential, in any form including, but not limited to, proprietary information and trade secrets, whether or not protected under any patent, copy right or other intellectual property laws, in any oral, photographic or electronic form, whether contained on computer hard disks or floppy diskettes or otherwise without any limitation whatsoever. Without prejudice to the generality of the foregoing, the Confidential Information shall include all information about the party and its customers, costing and technical data, studies, consultants reports, financial information, computer models and programs, software Code, contracts, drawings, blue prints, specifications, operating techniques, processes, models, diagrams, data sheets, reports and other information with respect to any of the foregoing matters. All and every information received by the parties and marked confidential hereto shall be assumed to be confidential information unless otherwise proved. It is further agreed that the information relating to the Bank and its customers is deemed confidential whether marked confidential or not.

14.2 All information relating to the accounts of the Bank's customers shall be confidential information, whether labeled as such or otherwise.

14.3 All information relating to the infrastructure and Applications (including designs and processes) shall be deemed to be Confidential Information whether labeled as such or not. Service Provider personnel/resources responsible for the project are expected to take care that their representatives, where necessary, have executed a Non-Disclosure Agreement similar to comply with the confidential obligations under this Agreement.

14.4 Each party agrees that it will not disclose any Confidential Information received from the other to any third parties under any circumstances without the prior written consent of the other party unless such disclosure of Confidential

Information is required by law, legal process or any order of any government authority. Service Provider in this connection, agrees to abide by the laws especially applicable to confidentiality of information relating to customers of Banks and the banks per-se, even when the disclosure is required under the law. In such event, the Party must notify the other Party that such disclosure has been made in accordance with law; legal process or order of a government authority.

14.5 Each party, including its personnel, shall use the Confidential Information only for the purposes of achieving objectives set out in this Agreement. Use of the Confidential Information for any other purpose shall constitute breach of trust of the same.

14.6 Each party may disclose the Confidential Information to its personnel solely for the purpose of undertaking work directly related to the Agreement. The extent of Confidential Information disclosed shall be strictly limited to what is necessary for those particular personnel to perform his/her duties in connection with the Agreement. Further each Party shall ensure that each personnel representing the respective party agree to be bound by obligations of confidentiality no less restrictive than the terms of this Agreement.

14.7 The non-disclosure obligations herein contained shall not be applicable only under the following circumstances:

(i) Where Confidential Information comes into the public domain during or after the date of this Agreement otherwise than by disclosure by a receiving party in breach of the terms hereof.

(ii) Where any Confidential Information was disclosed after receiving the written consent of the disclosing party.

(iii) Where receiving party is requested or required by law or by any Court or governmental agency or authority to disclose any of the Confidential Information, then receiving party will provide the other Party with prompt notice of such request or requirement prior to such disclosure.

(iv) Where any Confidential Information was received by the receiving party from a third party which does not have any obligations of confidentiality to the other Party.

(v) Where Confidential Information is independently developed by receiving party without any reference to or use of disclosing party's Confidential Information.

14.8 Receiving party undertakes to promptly notify disclosing party in writing any breach of obligation of the Agreement by its employees or representatives including confidentiality obligations. Receiving party acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that disclosing party shall be entitled, without waiving any other rights or remedies, to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.

14.9 Service Provider shall ensure to filter all phishing / spamming / overflow attacks in order to ensure availability and integrity on continuous basis.

14.10 Service Provider shall not, without the Bank's prior written consent, make use of any document or information received from the Bank except for purposes of performing the Services and obligations under this Agreement.

14.11 Any document received from the Bank shall remain the property of the Bank and shall be returned (in all copies) to the Bank on completion of Service Provider's performance under the Agreement.

14.12 The Bank reserves its right to recall all the Bank's materials including Confidential Information, if stored in Service Provider system or environment, at any time during the term of this Agreement or immediately upon expiry or termination of Agreement. Service Provider shall ensure complete removal of such material or data from its system or environment (including backup media) to the satisfaction of the Bank.

14.13 The foregoing obligations (collectively referred to as "Confidentiality Obligations") set out in this Agreement shall survive the term of this Agreement and for a period of five (5) years thereafter provided Confidentiality Obligations with respect to individually identifiable information, customer's data of Parties or software in human-readable form (e.g., source code) shall survive in perpetuity.

15. OWNERSHIP

15.1 Service Provider agrees that the Bank owns the entire right, title and interest to any inventions, designs, discoveries, writings and works of authorship,

including all intellectual property rights, copyrights. Any work made under this Agreement shall be deemed to be 'work made for hire' under any Indian/U.S. or any other applicable copyright laws.

15.2 All information processed by Service Provider during Services belongs to the Bank. Service Provider shall not acquire any other right in respect of the information for the license to the rights owned by the Bank. Service Provider will implement mutually agreed controls to protect the information. Service Provider also agrees that it will protect the information appropriately.

16. TERMINATION

16.1 The Bank may, without prejudice to any other remedy for breach of Agreement, by written notice of not less than 30 (thirty) days, terminate the Agreement in whole or in part:

(e) If Service Provider fails to deliver any or all the obligations within the time period specified in the Agreement, or any extension thereof granted by the Bank;

(f) If Service Provider fails to perform any other obligation(s) under the Agreement;

(g) Violations of any terms and conditions stipulated in the RFP;

(h) On happening of any termination event mentioned herein above in this Agreement.

Prior to providing a written notice of termination to Service Provider under clause 16.1 (i) to 16.1 (iii), the Bank shall provide Service Provider with a written notice of 30 (thirty) days to cure such breach of the Agreement. If the breach continues or remains unrectified after expiry of cure period, the Bank shall have right to initiate action in accordance with above clause.

16.2 The Bank, by written notice of not less than 90 (ninety) days, may terminate the Agreement, in whole or in part, for its convenience, provided same shall not be invoked by the Bank before completion of half of the total Contract period (including the notice period). In the event of termination of the Agreement for the Bank's convenience, Service Provider shall be entitled to

receive payment for the Services rendered (delivered) up to the effective date of termination.

16.3 In the event the Bank terminates the Agreement in whole or in part for the breaches attributable to Service Provider, the bank may procure, upon such terms and in such manner, as it deems appropriate, Services similar to those undelivered and subject to clause 20 Service Provider shall be liable to the Bank for any increase in costs for such similar Services. However, Service Provider, in case of part termination, shall continue the performance of the Agreement to the extent not terminated.

16.4 The Bank shall have a right to terminate the Agreement immediately by giving a notice in writing to Service Provider in the following eventualities:

(i) If any Receiver/Liquidator is appointed in connection with the business of the Service Provider or Service Provider transfers substantial assets in favour of its creditors or any orders / directions are issued by any Authority / Regulator which has the effect of suspension of the business of Service Provider.

(ii) If Service Provider applies to the Court or passes a resolution for voluntary winding up of or any other creditor / person files a petition for winding up or dissolution of Service Provider.

(iii) If any acts of commission or omission on the part of Service Provider or its agents, employees, sub-contractors or representatives, in the reasonable opinion of the Bank tantamount to fraud or prejudicial to the interest of the Bank or its employees.

(iv) Any document, information, data or statement submitted by Service Provider in response to RFP, based on which Service Provider was considered eligible or successful, is found to be false, incorrect or misleading.

16.5 In the event of the termination of the Agreement Service Provider shall be liable and responsible to return to the Bank all records, documents, data and information including Confidential Information pertains to or relating to the Bank in its possession.

16.6 In the event of termination of the Agreement for material breach, the Bank shall have the right to report such incident in accordance with the mandatory reporting obligations under the applicable law or regulations.

16.7 Upon termination or expiration of this Agreement, all rights and obligations of the Parties hereunder shall cease, except such rights and obligations as may have accrued on the date of termination or expiration; the obligation of indemnity; obligation of payment; confidentiality obligation; Governing Law clause; Dispute resolution clause; and any right which a Party may have under the applicable Law.

17. DISPUTE REDRESSAL MACHANISM & GOVERNING LAW

17.1 All disputes or differences whatsoever arising between the parties out of or in connection with this Agreement (including dispute concerning interpretation) or in discharge of any obligation arising out of the Agreement (whether during the progress of work or after completion of such work and whether before or after the termination of this Agreement, abandonment or breach of this Agreement), shall be settled amicably.

17.2 If the parties are not able to solve them amicably within 30 (thirty) days after dispute occurs as evidenced through the first written communication from any party notifying the other regarding the disputes, either party (the Bank or Service Provider) shall give written notice to other party clearly setting out there in, specific dispute(s) and/or difference(s), and shall be referred to a sole arbitrator mutually agreed upon, and the award made in pursuance thereof shall be binding on the parties.

17.3 In the absence of consensus about the single arbitrator, the dispute may be referred to an arbitration panel; one to be nominated by each party and the said arbitrators shall nominate a presiding arbitrator, before commencing the arbitration proceedings. The arbitration shall be settled in accordance with the applicable Indian Laws and the arbitration shall be conducted in accordance with the Arbitration and Conciliation Act, 1996.

17.4 Service Provider shall continue work under the Agreement during the arbitration proceedings, unless otherwise directed by the Bank or unless the

matter is such that the work cannot possibly be continued until the decision of the arbitrator is obtained.

17.5 Arbitration proceeding shall be held at **Mumbai**, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be in English.

17.6 This Agreement shall be governed by laws in force in India. Subject to the arbitration clause above, all disputes arising out of or in relation to this Agreement, shall be subject to the exclusive jurisdiction of the courts at **Mumbai** only.

17.7 In case of any change in applicable laws that has an effect on the terms of this Agreement, the Parties agree that the Agreement may be reviewed, and if deemed necessary by the Parties, make necessary amendments to the Agreement by mutual agreement in good faith, in case of disagreement obligations mentioned in this clause shall be observed.

18. POWERS TO VARY OR OMIT WORK

18.1 No alterations, amendments, omissions, additions, suspensions or variations of the work (hereinafter referred to as variation) under the Agreement shall be made by Service provider except as directed in writing by Bank. The Bank shall have full powers, subject to the provision herein after contained, from time to time during the execution of the Agreement, by notice in writing to instruct Service provider to make any variation without prejudice to the Agreement. Service provider shall carry out such variations and be bound by the same conditions, though the said variations occurred in the Agreement documents. If any suggested variations would, in the opinion of Service provider, if carried out, prevent them from fulfilling any of their obligations under the Agreement, they shall notify the Bank, thereof, in writing with reasons for holding such opinion and Bank shall instruct Service provider to make such other modified variation without prejudice to the Agreement. Service provider shall carry out such variations and be bound by the same conditions, though the said variations occurred in the Agreement documents. If Bank confirms their instructions Service provider's obligations will be modified to such an extent as may be mutually agreed. If such variation involves extra cost, any agreed difference in

cost occasioned by such variation shall be mutually agreed between the parties. In any case in which Service provider has received instructions from the Bank as to the requirement of carrying out the altered or additional substituted work, which either then or later on, will in the opinion of Service provider, involve a claim for additional payments, such additional payments shall be mutually agreed in line with the terms and conditions of the order.

18.2 If any change in the work is likely to result in reduction in cost, the parties shall agree in writing so as to the extent of reduction in payment to be made to Service Provider, before Service provider proceeding with the change.

19. WAIVER OF RIGHTS

Each Party agrees that any delay or omission on the part of the other Party to exercise any right, power or remedy under this Agreement will not automatically operate as a waiver of such right, power or remedy or any other right, power or remedy and no waiver will be effective unless it is in writing and signed by the waiving Party. Further the waiver or the single or partial exercise of any right, power or remedy by either Party hereunder on one occasion will not be construed as a bar to a waiver of any successive or other right, power or remedy on any other occasion.

20. LIMITATION OF LIABILITY

20.1 The maximum aggregate liability of Service Provider, subject to clause 20.3, in respect of any claims, losses, costs or damages arising out of or in connection with this Agreement shall not exceed the total Project Cost.

20.2 Under no circumstances shall either Party be liable for any indirect, consequential or incidental losses, damages or claims including loss of profit, loss of business or revenue.

20.3 The limitations set forth in Clause 20.1 shall not apply with respect to:

(i) claims that are the subject of indemnification pursuant to Clause 12[12] (infringement of third party Intellectual Property Right);

(ii) damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider;

[12] Please see Clause 12 'IPR Indemnification'

(iii) damage(s) occasioned by Service Provider for breach of Confidentiality Obligations;

(iv) Regulatory or statutory fines imposed by a Government or Regulatory agency for non-compliance of statutory or regulatory guidelines applicable to the Bank, provided such guidelines were brought to the notice of Service Provider.

For the purpose of clause 20.3(ii) "Gross Negligence" means any act or failure to act by a party which was in reckless disregard of or gross indifference to the obligation of the party under this Agreement and which causes injury, damage to life, personal safety, real property, harmful consequences to the other party, which such party knew, or would have known if it was acting as a reasonable person, would result from such act or failure to act for which such Party is legally liable. Notwithstanding the forgoing, Gross Negligence shall not include any action taken in good faith. "Willful Misconduct" means any act or failure to act with an intentional disregard of any provision of this Agreement, which a party knew or should have known if it was acting as a reasonable person, which would result in injury, damage to life, personal safety, real property, harmful consequences to the other party, but shall not include any error of judgment or mistake made in good faith.

21. FORCE MAJEURE

21.1 Notwithstanding anything else contained in the Agreement, neither Party shall be liable for any delay in performing its obligations herein if and to the extent that such delay is the result of an event of Force Majeure.

21.2 For the purposes of this clause, 'Force Majeure' means and includes wars, insurrections, revolution, civil disturbance, riots, terrorist acts, public strikes, hartal, bundh, fires, floods, epidemic, quarantine restrictions, freight embargoes, declared general strikes in relevant industries, Vis Major, acts of Government in their sovereign capacity, impeding reasonable performance of Service Provider and / or sub-contractor but does not include any foreseeable

events, commercial considerations or those involving fault or negligence on the part of the party claiming Force Majeure.

21.3 If Force Majeure situation arises, the non-performing Party shall promptly notify to the other Party in writing of such conditions and the cause(s) thereof. Unless otherwise agreed in writing, the non-performing Party shall continue to perform its obligations under the Agreement as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

21.4 If the Force Majeure situation continues beyond 30 (thirty) days, either Party shall have the right to terminate the Agreement by giving a notice to the other Party. Neither Party shall have any penal liability to the other in respect of the termination of this Agreement as a result of an event of Force Majeure. However, Service Provider shall be entitled to receive payments for all services actually rendered up to the date of the termination of this Agreement.

22. NOTICES

22.1 Any notice or any other communication required to be given under this Agreement shall be in writing and may be given by delivering the same by hand or sending the same by prepaid registered mail, postage prepaid, telegram or facsimile to the relevant address set forth below or such other address as each Party may notify in writing to the other Party from time to time. Any such notice given as aforesaid shall be deemed to be served or received at the time upon delivery (if delivered by hand) or upon actual receipt (if given by postage prepaid, telegram or facsimile).

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

22.3 The addresses for Communications to the Parties are as under.

(a) In the case of the Bank

Deputy General Manager
IT-Platform Engineering-I Department,
State Bank of India Global IT Centre,
Gr Floor 'A'- Wing, Plot no 8/9/10,
Sector -11, CBD Belapur
Navi Mumbai- 400614

(b) In case of Service Provider

_____

_____

_____

_____

_____

22.4 In case there is any change in the address of one Party, it shall be promptly communicated in writing to the other Party.

23. GENERAL TERMS & CONDITIONS

23.1 PUBLICITY: Service Provider may make a reference of the services rendered to the Bank covered under this Agreement on Service provider's Web Site or in their sales presentations, promotional materials, business plans or news releases etc., only after prior written approval from the Bank.

23.2 SUCCESSORS AND ASSIGNS: This Agreement shall bind and inure to the benefit of the parties, and their respective successors and permitted assigns.

23.3 NON-HIRE AND NON-SOLICITATION: During the term of this Agreement and for a period of one year thereafter, neither party shall (either directly or indirectly through a third party) employ, solicit to employ, cause to be solicited for the purpose of employment or offer employment to any employee(s) of the other party, or aid any third person to do so, without the specific written consent of the other party. However nothing in this clause shall affect the Bank's regular recruitments as per its recruitment policy and not targeted to the employees of Service provider.

23.4 SEVERABILITY: The invalidity or unenforceability of any provision of this Agreement shall not in any way effect, impair or render unenforceable this Agreement or any other provision contained herein, which shall remain in full force and effect.

23.5 MODIFICATION: This Agreement may not be modified or amended except in writing signed by duly authorized representatives of each party with express mention thereto of this Agreement.

23.6 ENTIRE AGREEMENT: The following documents along with all addenda issued thereto shall be deemed to form and be read and construed as integral part of this Agreement and in case of any contradiction between or among them the priority in which a document would prevail over another would be as laid down below beginning from the highest priority to the lowest priority:

(i) This Agreement;

(ii) Annexure of Agreement;

(iii) Purchase Order No._____ dated _____; and

(iv) RFP

23.7 PRIVITY: Neither this Agreement nor any provision hereof is intended to confer upon any person/s other than the Parties to this Agreement any rights or remedies hereunder.

23.8 DUE AUTHORISATION: Each of the undersigned hereby represents to the other that she/ he is authorized to enter into this Agreement and bind the respective parties to this Agreement.

23.9 COUNTERPART: This Agreement is executed in duplicate and each copy is treated as original for all legal purposes.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives as of the date and day first mentioned above.

State Bank of India	**_____Service Provider**
By:	**By:**
Name:	**Name:**
Designation:	**Designation:**
Date:	**Date:**
WITNESS:	
1.	1.
2.	2.

SLA-ANNEXURE-A

SCOPE OF WORK

As mention in Appendix-E "SCOPE of Work and Payment Schedule" of the RFP no. SBI/GITC/Platform Engineering-I/2021/2022/809 Dated: 06-Dec-2021

SLA-ANNEXURE-B

(a) INFRASTUCTURE SUPPORT METRICS

Service Area	**SLA measurement**	**Penalty of 10% on Monthly Support Services bill, Maximum 10% on Yearly bill**		**Calculate penalty on**
		0 %	**1% for every 1% shortfall from the stipulated service level**	
Help Desk	Time taken for resolution of calls. (99.9% of the calls should be resolved within the stipulated response time)	More than or equal to 99.9 % of service level	Less than 99.9 % of service level	10% Penalty will be deducted on Yearly support Services Payment after breach of SLA

SLA-ANNEXURE-C

SERVICE DESK SUPPORT METRIC

AS MENTIONED IN APPENDIX-I OF THE RFP NO. SBI/GITC/Platform Engineering-I/2021/2022/809 Dated: 06-Dec-2021

SERVICE REVIEW MEETING Service Review meeting shall be held annually/half yearly. The following comprise of the Service Review Board:

Service Review meeting shall be held annually/ half yearly. The following comprise of the Service Review Board: ▪ President, SBI, DGM PE-I Department ▪ Members Project Owner Department , Service Integrator project team and OEM team

SLA ANNEXURE-D

Service Integrator shall provide the escalation matrix for their organization as well as OEMs. SI is also responsible for review the escalation matric on half yearly basis and update the matrix as and when required. The format for escalation matrix is as under.

Service level Category	Response/Resolution Time	Escalation thresholds			
		Escalation Level 1		Escalation.....	
		Escalation to	Escalation Mode	Escalation to	Escalation Mode
Production Support		<Name, designation contact no.>			
Service Milestones		<Name, designation contact no.>			
Infrastructure Management		<Name, designation contact no.>			
Application Development & Maintenance		<Name, designation contact no.>			
Service Desk Support		<Name, designation contact no.>			

SLA-ANNEXURE-E

PENALTIES FOR SERVICE LEVEL AGGREMENT

AS MENTIONED IN APPENDIX-I OF THE RFP NO. SBI/GITC/Platform Engineering-I/2021/2022/809 Dated: 06-Dec-2021

SLA ANNEXURE-F

Transition & Knowledge Transfer Plan

1. Introduction

1.1 This Annexure describes the duties and responsibilities of Service Provider and the Bank to ensure proper transition of services and to ensure complete knowledge transfer.

2. Objectives

2.1 The objectives of this annexure are to:

(1) ensure a smooth transition of Services from Service Provider to a New/Replacement SERVICE PROVIDER or back to the Bank at the termination or expiry of this Agreement;

(2) ensure that the responsibilities of both parties to this Agreement are clearly defined in the event of exit and transfer; and

(3) ensure that all relevant Assets are transferred.

3. General

3.1 Where the Bank intends to continue equivalent or substantially similar services to the Services provided by Service Provider after termination or expiry the Agreement, either by performing them itself or by means of a New/Replacement SERVICE PROVIDER, Service Provider shall ensure the smooth transition to the Replacement SERVICE PROVIDER and shall co-operate with the Bank or the Replacement SERVICE PROVIDER as required in order to fulfil the obligations under this annexure.

3.2 Service Provider shall co-operate fully with the Bank and any potential Replacement SERVICE PROVIDERs tendering for any Services, including the transfer of responsibility for the provision of the Services previously performed by Service Provider to be achieved with the minimum of disruption. In particular:

3.2.1 during any procurement process initiated by the Bank and in anticipation of the expiry or termination of the Agreement and irrespective of the identity of any potential or actual Replacement SERVICE PROVIDER, Service Provider shall comply with all reasonable requests by the Bank to provide information relating to the operation of the Services, including but not limited to, hardware and

software used, inter-working, coordinating with other application owners, access to and provision of all performance reports, agreed procedures, and any other relevant information (including the configurations set up for the Bank and procedures used by Service Provider for handling Data) reasonably necessary to achieve an effective transition, provided that:

3.2.1.1 Service Provider shall not be obliged to provide any information concerning the costs of delivery of the Services or any part thereof or disclose the financial records of Service Provider to any such party;

3.2.1.2 Service Provider shall not be obliged to disclose any such information for use by an actual or potential Replacement SERVICE PROVIDER unless such a party shall have entered into a confidentiality agreement; and

3.2.1.3 whilst supplying information as contemplated in this paragraph 3.2.1 Service Provider shall provide sufficient information to comply with the reasonable requests of the Bank to enable an effective tendering process to take place but shall not be required to provide information or material which Service Provider may not disclose as a matter of law.

3.3 In assisting the Bank and/or the Replacement SERVICE PROVIDER to transfer the Services the following commercial approach shall apply:

(1) where Service Provider does not have to utilise resources in addition to those normally used to deliver the Services prior to termination or expiry, Service Provider shall make no additional Charges. The Bank may reasonably request that support and materials already in place to provide the Services may be redeployed onto work required to effect the transition provided always that where the Bank agrees in advance that such redeployment will prevent Service Provider from meeting any Service Levels, achieving any other key dates or from providing any specific deliverables to the Bank, the Bank shall not be entitled to claim any penalty or liquidated damages for the same.

(2) where any support and materials necessary to undertake the transfer work or any costs incurred by Service Provider are additional to those in place as part of the proper provision of the Services the Bank shall pay Service Provider for staff time agreed in advance at the rates agreed between the parties and

for materials and other costs at a reasonable price which shall be agreed with the Bank.

3.4 If so required by the Bank, on the provision of no less than 15 (fifteen) days' notice in writing, Service Provider shall continue to provide the Services or an agreed part of the Services for a period not exceeding **6 (Six)** months beyond the date of termination or expiry of the Agreement. In such event the Bank shall reimburse Service Provider for such elements of the Services as are provided beyond the date of termination or expiry date of the Agreement on the basis that:

(1) Services for which rates already specified in the Agreement shall be provided on such rates;

(2) materials and other costs, if any, will be charged at a reasonable price which shall be mutually agreed between the Parties.

3.5 Service Provider shall provide to the Bank an analysis of the Services to the extent reasonably necessary to enable the Bank to plan migration of such workload to a Replacement SERVICE PROVIDER provided always that this analysis involves providing performance data already delivered to the Bank as part of the performance monitoring regime.

3.6 Service Provider shall provide such information as the Bank reasonably considers to be necessary for the actual Replacement SERVICE PROVIDER, or any potential Replacement SERVICE PROVIDER during any procurement process, to define the tasks which would need to be undertaken in order to ensure the smooth transition of all or any part of the Services.

3.7 Service Provider shall make available such Key Personnel who have been involved in the provision of the Services as the Parties may agree to assist the Bank or a Replacement SERVICE PROVIDER (as appropriate) in the continued support of the Services beyond the expiry or termination of the Agreement, in which event the Bank shall pay for the services of such Key Personnel on a time and materials basis at the rates agreed between the parties.

3.8 Service Provider shall co-operate with the Bank during the handover to a Replacement SERVICE PROVIDER and such co-operation shall extend to, but shall not be limited to, inter-working, co-ordinating and access to and provision of all operational and performance documents, reports, summaries produced by Service Provider for the Bank, including the configurations set up for the Bank

and any and all information to be provided by Service Provider to the Bank under any other term of this Agreement necessary to achieve an effective transition without disruption to routine operational requirements.

4. Replacement SERVICE PROVIDER

4.1 In the event that the Services are to be transferred to a Replacement SERVICE PROVIDER, the Bank will use reasonable endeavors to ensure that the Replacement SERVICE PROVIDER co-operates with Service Provider during the handover of the Services.

5. Subcontractors

5.1 Service Provider agrees to provide the Bank with details of the Subcontracts (if permitted by the Bank) used in the provision of the Services. Service Provider will not restrain or hinder its Subcontractors from entering into agreements with other prospective service providers for the delivery of supplies or services to the Replacement SERVICE PROVIDER.

6. Transfer of Configuration Management Database

6.1 6 (six) months prior to expiry or within 2 (two) week of notice of termination of this Agreement Service Provider shall deliver to the Bank a full, accurate and up to date cut of content from the Configuration Management Database (or equivalent) used to store details of Configurable Items and Configuration Management data for all products used to support delivery of the Services.

7. Transfer of Assets

7.1 6 (six) months prior to expiry or within 2 (two) week of notice of termination of the Agreement Service Provider shall deliver to the Bank the Asset Register comprising:

(1) a list of all Assets eligible for transfer to the Bank; and

(2) a list identifying all other Assets, (including human resources, skillset requirement and know-how), that are ineligible for transfer but which are essential to the delivery of the Services. The purpose of each component and the reason for ineligibility for transfer shall be included in the list.

7.2 Within 1 (one) month of receiving the Asset Register as described above, the Bank shall notify Service Provider of the Assets it requires to be transferred, (the

"Required Assets"), and the Bank and Service Provider shall provide for the approval of the Bank a draft plan for the Asset transfer.

7.3 In the event that the Required Assets are not located on Bank premises:

(1) Service Provider shall be responsible for the dismantling and packing of the Required Assets and to ensure their availability for collection by the Bank or its authorised representative by the date agreed for this;

(2) any charges levied by Service Provider for the Required Assets not owned by the Bank shall be fair and reasonable in relation to the condition of the Assets and the then fair market value; and

(3) for the avoidance of doubt, the Bank will not be responsible for the Assets.

7.4 Service Provider warrants that the Required Assets and any components thereof transferred to the Bank or Replacement SERVICE PROVIDER benefit from any remaining manufacturer's warranty relating to the Required Assets at that time, always provided such warranties are transferable to a third party.

8. Transfer of Documentation

8.1 6 (six) months prior to expiry or within 2 (two) weeks of notice of termination of this Agreement Service Provider shall deliver to Bank a full, accurate and up-to date set of Documentation that relates to any element of the Services as defined in Annexure A.

9. Transfer of Service Management Process

9.1 6 (six) months prior to expiry or within 2 (two) weeks of notice of termination of this Agreement Service Provider shall deliver to the Bank:

(a) a plan for the handover and continuous delivery of the Service Desk function and allocate the required resources;

(b) full and up to date, both historical and outstanding Service Desk ticket data including, but not limited to:

(1) Incidents;

(2) Problems;

(3) Service Requests;

(4) Changes;

(5) Service Level reporting data;

(c) a list and topology of all tools and products associated with the provision of the Software and the Services;

(d) full content of software builds and server configuration details for software deployment and management; and

(e) monitoring software tools and configuration.

10. Transfer of Knowledge Base

10.1 6 (six) months prior to expiry or within 2 (two) week of notice of termination of this Agreement Service Provider shall deliver to the Bank a full, accurate and up to date cut of content from the knowledge base (or equivalent) used to troubleshoot issues arising with the Services but shall not be required to provide information or material which Service Provider may not disclose as a matter of law.

11. Transfer of Data

11.1 In the event of expiry or termination of this Agreement Service Provider shall cease to use the Bank's Data and, at the request of the Bank, shall destroy all such copies of the Bank's Data then in its possession to the extent specified by the Bank.

11.2 Except where, pursuant to paragraph 11.1 above, the Bank has instructed Service Provider to destroy such Bank's Data as is held and controlled by Service Provider, 1 (one) months prior to expiry or within 1 (one) month of termination of this Agreement, Service Provider shall deliver to the Bank:

(1) An inventory of the Bank's Data held and controlled by Service Provider, plus any other data required to support the Services; and/or

(2) a draft plan for the transfer of the Bank's Data held and controlled by Service Provider and any other available data to be transferred.

12. Training Services on Transfer

12.1 Service Provider shall comply with the Bank's reasonable request to assist in the identification and specification of any training requirements following expiry or termination. The purpose of such training shall be to enable the Bank or a Replacement SERVICE PROVIDER to adopt, integrate and utilize the Data and Assets transferred and to deliver an equivalent service to that previously provided by Service Provider.

12.2 The provision of any training services and/or deliverables and the charges for such services and/or deliverables shall be agreed between the parties.

12.3 Subject to paragraph 12.2 above, Service Provider shall produce for the Bank's consideration and approval 6 (six) months prior to expiry or within 10 (ten) working days of issue of notice of termination:

(1) A training strategy, which details the required courses and their objectives;

(2) Training materials (including assessment criteria); and

(3) a training plan of the required training events.

12.4 Subject to paragraph 12.2 above, Service Provider shall schedule all necessary resources to fulfil the training plan, and deliver the training as agreed with the Bank.

13. Transfer Support Activities

13.1 6 (six) months prior to expiry or within 10 (ten) Working Days of issue of notice of termination, Service Provider shall assist the Bank or Replacement SERVICE PROVIDER to develop a viable exit transition plan which shall contain details of the tasks and responsibilities required to enable the transition from the Services provided under this Agreement to the Replacement SERVICE PROVIDER or the Bank, as the case may be.

13.2 The exit transition plan shall be in a format to be agreed with the Bank and shall include, but not be limited to:

(1) a timetable of events;

(2) resources;

(3) assumptions;

(4) activities;

(5) responsibilities; and

(6) risks.

13.3 Service Provider shall supply to the Bank or a Replacement SERVICE PROVIDER specific materials including but not limited to:

(a) Change Request log;

(b) entire back-up history; and

(c) dump of database contents including the Asset Register, problem management system and operating procedures. For the avoidance of doubt this shall not include proprietary software tools of Service Provider which are used for project management purposes generally within Service Provider's business.

13.4 Service Provider shall supply to the Bank or a Replacement SERVICE PROVIDER proposals for the retention of Key Personnel for the duration of the transition period.

13.5 On the date of expiry Service Provider shall provide to the Bank refreshed versions of the materials required under paragraph 13.3 above which shall reflect the position as at the date of expiry.

13.6 Service Provider shall provide to the Bank or to any Replacement SERVICE PROVIDER within 14 (fourteen) Working Days of expiry or termination a full and complete copy of the Incident log book and all associated documentation recorded by Service Provider till the date of expiry or termination.

13.7 Service Provider shall provide for the approval of the Bank a draft plan to transfer or complete work-in-progress at the date of expiry or termination.

14. Use of STATE BANK OF INDIA Premises

14.1 Prior to expiry or on notice of termination of this Agreement, Service Provider shall provide for the approval of the Bank a draft plan specifying the necessary steps to be taken by both Service Provider and the Bank to ensure that the Bank's Premises are vacated by Service Provider.

14.2 Unless otherwise agreed, Service Provider shall be responsible for all costs associated with Service Provider's vacation of the Bank's Premises, removal of equipment and furnishings, redeployment of Service Provider Personnel, termination of arrangements with Subcontractors and service contractors and restoration of the Bank Premises to their original condition (subject to a reasonable allowance for wear and tear).

XXXXX

SLA Template End

Appendix–K

NON-DISCLOSURE AGREEMENT

THIS RECIPROCAL NON-DISCLOSURE AGREEMENT (the "Agreement") is made at _____ between:

State Bank of India constituted under the State Bank of India Act, 1955 having its Corporate Centre and Central Office at State Bank Bhavan, Madame Cama Road, Nariman Point, Mumbai-21 and its Global IT Centre at Sector-11, CBD Belapur, Navi Mumbai- 400614 through its _____ Department (hereinafter referred to as "Bank" which expression includes its successors and assigns) of the ONE PART;

And

_____ a private/public limited company/LLP/Firm *<strike off whichever is not applicable>* incorporated under the provisions of the Companies Act, 1956/ Limited Liability Partnership Act 2008/ Indian Partnership Act 1932 *<strike off whichever is not applicable>*, having its registered office at _____ (hereinafter referred to as "_____" which expression shall unless repugnant to the subject or context thereof, shall mean and include its successors and permitted assigns) of the OTHER PART;

And Whereas

1. _____ is carrying on business of providing _____, has agreed to _____ for the Bank and other related tasks.

3. For purposes of advancing their business relationship, the parties would need to disclose certain valuable confidential information to each other (the Party receiving the information being referred to as the "Receiving Party" and the Party disclosing the information being referred to as the "Disclosing Party. Therefore, in consideration of covenants and agreements contained herein for the mutual disclosure of confidential information to each other, and intending to be legally bound, the parties agree to terms and conditions as set out hereunder.

NOW IT IS HEREBY AGREED BY AND BETWEEN THE PARTIES AS UNDER

1. **Confidential Information and Confidential Materials:**

(a) "Confidential Information" means non-public information that Disclosing Party designates as being confidential or which, under the circumstances surrounding disclosure ought to be treated as confidential. "Confidential Information" includes,

without limitation, information relating to developed, installed or purchased Disclosing Party software or hardware products, the information relating to general architecture of Disclosing Party's network, information relating to nature and content of data stored within network or in any other storage media, Disclosing Party's business policies, practices, methodology, policy design delivery, and information received from others that Disclosing Party is obligated to treat as confidential. Confidential Information disclosed to Receiving Party by any Disclosing Party Subsidiary and/ or agents is covered by this agreement

(b) Confidential Information shall not include any information that: (i) is or subsequently becomes publicly available without Receiving Party's breach of any obligation owed to Disclosing party; (ii) becomes known to Receiving Party free from any confidentiality obligations prior to Disclosing Party's disclosure of such information to Receiving Party; (iii) became known to Receiving Party from a source other than Disclosing Party other than by the breach of an obligation of confidentiality owed to Disclosing Party and without confidentiality restrictions on use and disclosure; or (iv) is independently developed by Receiving Party.

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

2. **Restrictions**

(a) Each party shall treat as confidential the Contract and any and all information ("confidential information") obtained from the other pursuant to the Contract and shall not divulge such information to any person (except to such party's "Covered Person" which term shall mean employees, contingent workers and professional advisers of a party who need to know the same) without the other party's written consent provided that this clause shall not extend to information which was rightfully in the possession of such party prior to the commencement of the negotiations leading to the Contract, which is already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this clause). Receiving Party will have executed or shall execute appropriate written agreements with Covered Person, sufficient to enable it to comply with all the provisions of this Agreement. If Service Provider appoints any Sub-Contractor (if allowed) then Service Provider may disclose confidential information to such Sub-Contractor subject to such Sub Contractor giving the Bank an undertaking in similar terms to the provisions of this clause. Any breach of this Agreement by Receiving Party's Covered Person or Sub-Contractor shall also be constructed a breach of this Agreement by Receiving Party.

(b) Receiving Party may disclose Confidential Information in accordance with judicial or other governmental order to the intended recipients (as detailed in this clause), provided Receiving Party shall give Disclosing Party reasonable notice (provided not restricted by applicable laws) prior to such disclosure and shall comply with any

applicable protective order or equivalent. The intended recipients for this purpose are:

i. the statutory auditors of the either party and

ii. government or regulatory authorities regulating the affairs of the parties and inspectors and supervisory bodies thereof

(c) Confidential Information and Confidential Material may be disclosed, reproduced, summarized or distributed only in pursuance of Receiving Party's business relationship with Disclosing Party, and only as otherwise provided hereunder. Receiving Party agrees to segregate all such Confidential Material from the confidential material of others in order to prevent mixing.

3. **Rights and Remedies**

(a) Receiving Party shall notify Disclosing Party immediately upon discovery of any unauthorized used or disclosure of Confidential Information and/ or Confidential Materials, or any other breach of this Agreement by Receiving Party, and will cooperate with Disclosing Party in every reasonable way to help Disclosing Party regain possession of the Confidential Information and/ or Confidential Materials and prevent its further unauthorized use.

(b) Receiving Party shall return all originals, copies, reproductions and summaries of Confidential Information or Confidential Materials at Disclosing Party's request, or at Disclosing Party's option, certify destruction of the same.

(c) Receiving Party acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that disclosing party shall be entitled, without waiving any other rights or remedies (including but not limited to as listed below), to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.

i. Suspension of access privileges

ii. Change of personnel assigned to the job.

iii. Termination of contract

(d) Disclosing Party may visit Receiving Party's premises, with reasonable prior notice and during normal business hours, to review Receiving Party's compliance with the term of this Agreement.

4. **Miscellaneous**

(a) All Confidential Information and Confidential Materials are and shall remain the sole and of Disclosing Party. By disclosing information to Receiving Party, Disclosing Party does not grant any expressed or implied right to Receiving Party to

disclose information under the Disclosing Party's patents, copyrights, trademarks, or trade secret information.

(b) Confidential Information made available is provided "As Is," and disclosing party disclaims all representations, conditions and warranties, express or implied, including, without limitation, representations, conditions or warranties of accuracy, completeness, performance, fitness for a particular purpose, satisfactory quality and merchantability provided same shall not be construed to include fraud or wilful default of disclosing party.

(c) Neither party grants to the other party any license, by implication or otherwise, to use the Confidential Information, other than for the limited purpose of evaluating or advancing a business relationship between the parties, or any license rights whatsoever in any patent, copyright or other intellectual property rights pertaining to the Confidential Information.

(d) The terms of Confidentiality under this Agreement shall not be construed to limit either party's right to independently develop or acquire product without use of the other party's Confidential Information. Further, either party shall be free to use for any purpose the residuals resulting from access to or work with such Confidential Information, provided that such party shall maintain the confidentiality of the Confidential Information as provided herein. The term "residuals" means information in non-tangible form, which may be retained by person who has had access to the Confidential Information, including ideas, concepts, know-how or techniques contained therein. Neither party shall have any obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of residuals. However, the foregoing shall not be deemed to grant to either party a license under the other party's copyrights or patents.

(e) This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. It shall not be modified except by a written agreement dated subsequently to the date of this Agreement and signed by both parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of Disclosing Party, its agents, or employees, except by an instrument in writing signed by an authorized officer of Disclosing Party. No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.

(f) In case of any dispute, both the parties agree for neutral third party arbitration. Such arbitrator will be jointly selected by the two parties and he/she may be an auditor, lawyer, consultant or any other person of trust. The said proceedings shall be conducted in English language at Mumbai and in accordance with the provisions of Indian Arbitration and Conciliation Act 1996 or any Amendments or Re-enactments thereto. Nothing in this clause prevents a party from having recourse to a court of competent jurisdiction for the sole purpose of seeking a preliminary injunction or

any other provisional judicial relief it considers necessary to avoid irreparable damage. This Agreement shall be governed by and construed in accordance with the laws of Republic of India. Each Party hereby irrevocably submits to the exclusive jurisdiction of the courts of Mumbai.

(g) Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the parties, their successors and assigns.

(h) If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect.

(i) The Agreement shall be effective from _____ ("Effective Date") and shall be valid for a period of _____ year(s) thereafter (the "Agreement Term"). The foregoing obligations as to confidentiality shall survive the term of this Agreement and for a period of five (5) years thereafter provided confidentiality obligations with respect to individually identifiable information, customer's data of Parties or software in human-readable form (e.g., source code) shall survive in perpetuity.

5. **Suggestions and Feedback**

Either party from time to time may provide suggestions, comments or other feedback to the other party with respect to Confidential Information provided originally by the other party (hereinafter "feedback"). Both party agree that all Feedback is and shall be entirely voluntary and shall not in absence of separate agreement, create any confidentially obligation for the receiving party. However, the Receiving Party shall not disclose the source of any feedback without the providing party's consent. Feedback shall be clearly designated as such and, except as otherwise provided herein, each party shall be free to disclose and use such Feedback as it sees fit, entirely without obligation of any kind to other party. The foregoing shall not, however, affect either party's obligations hereunder with respect to Confidential Information of other party.

Dated this _____ day of _____ (Month) *20*__ at _____(place)

For and on behalf of _____

Name		
Designation		

Place		
Signature		

For and on behalf of _____

Name		
Designation		
Place		
Signature		

Appendix–L

Pre-Bid Query Format
(To be provide strictly in Excel format)

Vendor Name	Sl. No	RFP Page No	RFP Clause No.	Existing Clause	Query/Suggestions

Appendix–M

Format for Submission of Client References

To whosoever it may concern

Particulars	Details
Client Information	
Client Name	
Client address	
Name of the contact person and designation	
Phone number of the contact person	
E-mail address of the contact person	
Project Details	
Name of the Project	
Start Date	
End Date	
Current Status (In Progress / Completed)	
Size of Project	
Value of Work Order (In Lakh) (only single work order)	

Name & Signature of authorised signatory

Seal of Company

Appendix–N

PRE CONTRACT INTEGRITY PACT

(TO BE STAMPED AS AN AGREEMENT)

General

This pre-Bid pre-contract Agreement (hereinafter called the Integrity Pact) is made on _____ day of the month of 201 , between, on the one hand, the State Bank of India a body corporate incorporated under the State Bank of India Act, 1955 having its Corporate Centre at State Bank Bhavan, Nariman Point, Mumbai through its _____ _____ Department / Office at Global IT Center at CBD Belapur, 400614,
(hereinafter called the "BUYER", which expression shall mean and include, unless the context otherwise requires, its successors) of the First Part

And

M/s_____ represented by Shri_____, Chief Executive Officer/ Authorized signatory (hereinafter called the "BIDDER/Seller which expression shall mean and include, unless the context otherwise requires, its / his successors and permitted assigns of the Second Part.

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

WHEREAS the BIDDER is a private company/public company/Government undertaking/partnership/registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is an Office / Department of State Bank of India performing its functions on behalf of State Bank of India.

NOW, THEREFORE,

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

- Enabling the BUYER to obtain the desired service / product at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement; and

- Enabling BIDDERs to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the BUYER will commit to prevent corruption, in any farm, by its officials by following transparent procedures.

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

1. **Commitments of the BUYER**

1.1 The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, Bid evaluation, contracting or implementation process related to the contract.

1.2 The BUYER will, during the pre-contract stage, treat all BIDDERs alike, and will provide to all BIDDERs the same information and will not provide any such information to any particular BIDDER which could afford an advantage to that particular BIDDER in comparison to other B1DDERs.

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

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

2. **Commitments of BIDDERs**

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

2. 2 The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the

contract.

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

2.4 Wherever applicable, the BIDDER shall disclose the name and address of agents and representatives permitted by the Bid documents and Indian BIDDERs shall disclose their foreign principals or associates, if any.

2.5 The BIDDER confirms and declares that they have not made any payments to any agents/brokers or any other intermediary, in connection with this Bid/contract.

2.6 The BIDDER further confirms and declares to the BUYER that the BIDDER is the original vendors or service providers in respect of product / service covered in the Bid documents and the BIDDER has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER, nor has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

2.7 The BIDDER, at the earliest available opportunity, i.e. either while presenting the Bid or during pre-contract negotiations and in any case before opening the financial Bid and before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the BUYER or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

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

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

2.10 The BIDDER shall not use improperly, for purposes of competition or personal gain, or pass. on 'to° others, any -information provided by the BUYER as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.

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

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

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

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

3. **Previous Transgression**

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

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

4. **Earnest Money (Security Deposit)**

4.1 While submitting commercial Bid, the BIDDER shall deposit an amount (specified in RFP) as Earnest Money/Security Deposit, with the BUYER through any of the mode mentioned in the RFP / Bid document and no such mode is specified, by a Bank Draft or a Pay Order in favour of State Bank of India from any Bank including SBI . However payment of any such amount by way of Bank Guarantee, if so permitted as per Bid documents / RFP should be from any Scheduled Commercial Bank other than SBI and promising payment of the guaranteed sum to the BUYER on demand within three working days without any demur whatsoever and without seeking any reasons whatsoever. The demand for payment by the BUYER shall be treated as conclusive proof for making such payment to the BUYER.

4.2 Unless otherwise stipulated in the Bid document / RFP, the Earnest Money/Security Deposit shall be valid upto a period of five years or the complete conclusion of the contractual obligations to the complete satisfaction of both the BIDDER and the BUYER, including warranty period, whichever is later.

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

4.4 No interest shall be payable by the BUYER to the BIDDER on Earnest

Money/Security Deposit for the period of its currency.

5. **Sanctions for Violations**

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

(i) To immediately call off the pre contract negotiations without assigning any reason and without giving any compensation to the BIDDER. However, the proceedings with the other BIDDER(s) would continue, unless the BUYER desires to drop the entire process.

(ii) The Earnest Money Deposit (in pre-contract stage) and/or Security Deposit/Performance Bond (after the contract is signed) shall stand forfeited either fully or partially, as decided by the BUYER and the BUYER shall not be required to assign any reason therefore.

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

(iv) To recover all sums already paid by the BUYER, and in case of an Indian BIDDER with interest thereon at 2% higher than the prevailing Base Rate of State Bank of India, while in case of a BIDDER from a country other than India with interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the BIDDER from the BUYER in connection with any other contract for any other stores, such outstanding could also be utilized to recover the aforesaid sum and interest.

(v) To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the BIDDER, in order to recover the payments, already made by the BUYER, along with interest.

(vi) To cancel all or any other Contracts with the BIDDER. The BIDDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER.

(vii) To debar the BIDDER from participating in future bidding processes of the BUYER or any of its Subsidiaries for a minimum period of five years, which may be further extended at the discretion of the BUYER.

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

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

(x) Intimate to the CVC, IBA, RBI, as the BUYER deemed fit the details of such events for appropriate action by such authorities.

5.2 The BUYER will be entitled to take all or any of the actions mentioned at para

5.1(i) to (x) of this Pact also on the Commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defined in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

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

6. **Fall Clause**

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

7. **Independent Monitors**

7.1 The BUYER has appointed Independent Monitors (hereinafter referred to as Monitors) for this Pact in consultation with the Central Vigilance Commission (Names and Addresses of the Monitors to be given).

Name	Dr. Parvez Hayat	Ms. Minnie Mathew
Category	IPS (Retd.)	IAS (Retd.)
Contact Number	Mobile No. 9810134469	Mobile No. 9951035888
Email Id	phayatips@gmail.com	Minniemathew635@gmail.com

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

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

7.4 Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings. Parties signing this Pact shall not approach the Courts while representing the matters to Independent External Monitors and he/she will await their decision in the matter.

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

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

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

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

8. **Facilitation of Investigation**

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

9. **Law and Place of Jurisdiction**

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

10. **Other Legal Actions**

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

11. **Validity**

11.1 The validity of this Integrity Pact shall be from date of its signing and extend up to 5 years or the complete execution of the contract to the satisfaction of both the BUYER and the BIDDER/Seller, including warranty period, whichever is later. In case BIDDER is unsuccessful, this Integrity Pact shall expire after six months from the date of the signing of the contract, with the successful Bidder by the BUYER.

11.2 Should one or several provisions of this Pact turn out to be invalid; the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an

agreement to their original intentions.

12. The parties hereby sign this Integrity Pact at _____ on_____

For BUYER Name of the Officer. Designation Office / Department / Branch State Bank of India.	For BIDDER Chief Executive Officer/ Authorised Signatory Designation
Witness 1 2	Witness 1. 2.

Note: This agreement will require stamp duty as applicable in the State where it is executed or stamp duty payable as per Maharashtra Stamp Act, whichever is higher.

Appendix–O

FORMAT FOR OEM SECURED SOULTION CONFIRMATION

To:

Deputy General Manager
Platform Engineering-I Department,
State Bank of India Global IT Centre,
Gr Floor 'B'- Wing, Plot no 8/9/10,
Sector -11, CBD Belapur
Navi Mumbai- 400614

I/We hereby certify and confirming that the proposed ESS solution is fully secured for deployment in SBI. We also confirm that our software solution is regularly reviewed and audited by competent auditor firms on **half yearly/yearly/mention periodicity** basis as per our organization internal systems and procedures.

We will provide the ESS solution security review latest certificates as and when required by Bank during the contract period of 05 years.

Name & Signature of authorized signatory

Seal of Company

****End OF the RFP Document****