



REQUEST FOR PROPOSAL

FOR

Engaging CAT-I Competent ISSPs from GITC empanelled vendors and ISD empanelled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

**State Bank Global IT Centre
Information Security Department
'A'- Wing, Ground Floor
Sector 11, CBD Belapur
Navi Mumbai 400614
INDIA**

| | |
|-----------------|---|
| Document | Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department |
|-----------------|---|

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

| | |
|---------|---|
| RFP No. | SBI/GITC/ISD/2024-25/ISO/27 (RFP-1426) |
| Date | 07.02.2025 |
| Contact | Manisha (Chief Manager) |

1. 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: Manisha Designation: Chief Manager Email ID:Manisha.raj@sbi.co.in Contact Address: 8929903012 mail copy to be marked to agm2.isd@sbi.co.in admin.isd@sbi.co.in manisha.raj@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 from 07.02.2025 to 20.02.2025 |
| 3 | Last date for requesting clarification | Upto 10.00 AM on 13.02.2025 All communications regarding points / queries requiring clarifications shall be given in writing or by e-mail. |
| 4 | Pre - bid Meeting at (venue) | At 03.00 P.M. on 15.02.2025 at ISD, GITC, Belapur CBD, Navi Mumbai |
| 5 | Clarifications to queries raised at pre-bid meeting will be provided by the Bank. | On 18.02.2025 (6.00 PM) |
| 6 | Last date and time for Bid submission | Up to 12.00 P.M. on 20.02.2025 |
| 7 | Address for submission of Bids | https://etender.sbi/SBI |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

| | | |
|----|---|--|
| | <i>(Please incorporate details of e-Procurement Agency portal wherein online bid has to be submitted)</i> | |
| 8 | Date and Time of opening of Technical Bids | 1.00 P.M. on 20.02.2025 |
| 9 | Opening of Indicative Price Bids | On a subsequent date which will be communicated to such Bidders who qualify in the Technical Bid. |
| 10 | Reverse Auction | On a subsequent date which will be communicated to such Bidders who qualify in the Technical Bid. |
| 11 | Tender Fee | Nil |
| 12 | Earnest Money Deposit | Nil |
| 13 | Bank Guarantee | 5 % of the Project Cost Performance Security in form of BG should be valid for Two year(s) from the effective date of the Contract and can be further extended till the completion of the project |
| 14 | Price Validity from the date of price discovery | 180 days |
| 15 | Contact details of e-Procurement agency appointed for e-procurement | e-Procurement Technologies LTD – CMM15 E-mail ID: nandan.v@eptl.in Landline No. : 079 6813 6820, 6850, 6857, 6848 Official Mobile No. : 9081000427 Ravi Sheladiya ravi.s@auctiontiger.net 07968136856 |

Contents

| | | |
|-----|--|----|
| 1. | SCHEDULE OF EVENTS | 2 |
| 2. | INVITATION TO BID:..... | 6 |
| 3. | DISCLAIMER: | 7 |
| 4. | DEFINITIONS:..... | 8 |
| 5. | SCOPE OF WORK: | 9 |
| 6. | ELIGIBILITY AND TECHNICAL CRITERIA: | 9 |
| 7. | COST OF BID DOCUMENT:..... | 9 |
| 8. | CLARIFICATION AND AMENDMENTS ON RFP/PRE-BID MEETING: | 9 |
| 9. | CONTENTS OF BID DOCUMENT:..... | 10 |
| 10. | EARNEST MONEY DEPOSIT (EMD):..... | 10 |
| 11. | BID PREPARATION AND SUBMISSION: | 11 |
| 12. | DEADLINE FOR SUBMISSION OF BIDS: | 13 |
| 13. | MODIFICATION AND WITHDRAWAL OF BIDS:..... | 13 |
| 14. | PERIOD OF BID VALIDITY AND VALIDITY OF PRICE QUOTED IN REVERSE AUCTION (RA): | 14 |
| 15. | BID INTEGRITY:..... | 14 |
| 16. | BIDDING PROCESS/OPENING OF TECHNICAL BIDS: | 14 |
| 17. | TECHNICAL EVALUATION: | 15 |
| 18. | EVALUATION OF INDICATIVE PRICE BIDS AND FINALIZATION: | 16 |
| 19. | CONTACTING THE BANK: | 17 |
| 20. | POWERS TO VARY OR OMIT WORK: | 20 |
| 21. | WAIVER OF RIGHTS:..... | 20 |
| 22. | CONTRACT AMENDMENT: | 21 |
| 23. | BANK’S RIGHT TO ACCEPT ANY BID AND TO REJECT ANY OR ALL BIDS: | 21 |
| 24. | BANK GUARANTEE: | 21 |
| 25. | SERVICES:..... | 21 |
| 26. | PENALTIES: | 22 |
| 27. | RIGHT TO VERIFICATION:..... | 22 |
| 28. | RIGHT TO AUDIT: | 22 |
| 29. | SUBCONTRACTING: | 23 |
| 30. | VALIDITY OF AGREEMENT: | 23 |
| 31. | LIMITATION OF LIABILITY:..... | 23 |
| 32. | CONFIDENTIALITY:..... | 24 |
| 33. | DELAY IN SERVICE PROVIDER’S PERFORMANCE: | 24 |
| 34. | SERVICE PROVIDER’S OBLIGATIONS: | 25 |
| 35. | TECHNICAL DOCUMENTATION: | 26 |
| 36. | INTELLECTUAL PROPERTY RIGHTS AND OWNERSHIP: | 26 |
| 37. | LIQUIDATED DAMAGES:..... | 28 |
| 38. | CONFLICT OF INTEREST:..... | 28 |
| 39. | CODE OF INTEGRITY AND DEBARMENT/BANNING:..... | 30 |
| 40. | TERMINATION FOR DEFAULT: | 33 |
| 41. | FORCE MAJEURE:..... | 35 |
| 42. | TERMINATION FOR INSOLVENCY: | 36 |
| 43. | TERMINATION FOR CONVENIENCE: | 36 |
| 44. | DISPUTES / ARBITRATION (APPLICABLE IN CASE OF SUCCESSFUL BIDDER ONLY): | 36 |
| 45. | GOVERNING LANGUAGE: | 37 |
| 46. | APPLICABLE LAW:..... | 37 |
| 47. | TAXES AND DUTIES: | 37 |
| 48. | TAX DEDUCTION AT SOURCE:..... | 39 |
| 49. | TENDER FEE:NOT APPLICABLE..... | 39 |
| 50. | EXEMPTION OF EMD AND TENDER FEE: | 39 |

| | |
|--|------------|
| 51. NOTICES:..... | 40 |
| APPENDIX –A | 41 |
| APPENDIX-B | 45 |
| ANNEXURE C4 | 50 |
| APPENDIX-D..... | 51 |
| APPENDIX-F | 58 |
| APPENDIX-G | 60 |
| APPENDIX-H..... | 62 |
| APPENDIX-I | 65 |
| APPENDIX-J | 67 |
| 1. DEFINITIONS & INTERPRETATION | 71 |
| 2. SCOPE OF WORK | 74 |
| 3. FEES /COMPENSATION | 74 |
| 4. LIABILITIES/OBLIGATION | 77 |
| 5. REPRESENTATIONS &WARRANTIES | 79 |
| 6. GENERAL INDEMNITY | 81 |
| 7. CONTINGENCY PLANS..... | 81 |
| 8. TRANSITION REQUIREMENT..... | 82 |
| 9. LIQUIDATED DAMAGES | 82 |
| 10. RELATIONSHIP BETWEEN THE PARTIES | 83 |
| 11. SUB CONTRACTING | 84 |
| 12. INTELLECTUAL PROPERTY RIGHTS | 84 |
| 13. INSPECTION AND AUDIT | 85 |
| 14. CONFIDENTIALITY | 87 |
| 16. TERMINATION..... | 90 |
| 17. DISPUTE REDRESSAL MACHANISM & GOVERNING LAW..... | 92 |
| 19. WAIVER OF RIGHTS | 93 |
| 20. LIMITATION OF LIABILITY | 94 |
| 21. FORCE MAJEURE..... | 95 |
| 22. NOTICES | 96 |
| 23. GENERAL TERMS & CONDITIONS..... | 97 |
| ANNEXURE-A | 100 |
| ANNEXURE-B..... | 104 |
| ANNEXURE-C | 113 |
| APPENDIX–K | 129 |
| APPENDIX–L | 135 |
| APPENDIX–M | 136 |
| DETAILED SCOPE OF THE APPLICATIONS: IT-PE-II, IT-PE-III,IT-E&TA , IT-DWH, IT-BID, IT-MAB ANALYTICS, IT-FO, IT-DCR ,IT-OPST,IT-SF, IT-SP3 (FY 2024-25) | 137 |

2. INVITATION TO BID:

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 bids are invited by Information Security Department (ISD) for Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT-TRADE FINANCE (FY 2024-25) Department

- i. 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.
- ii. 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.
- iii. Address for submission of online Bids, contact details including email address for sending communications are given in Schedule of Events of this RFP.
- iv. The purpose of SBI behind this RFP is to seek a detailed technical and commercial proposal for procurement of the Services desired in this RFP.
- v. This RFP document shall not be transferred, reproduced or otherwise used for purpose other than for which it is specifically issued.
- vi. 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 Services 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 Services adhering to Bank’s requirements outlined in this RFP.

3. 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.

4. 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. **Annual Maintenance Contract (AMC)** - It would be the annual cost of maintenance/upkeep/update of product or specified hardware and software.

5. SCOPE OF WORK:

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

6. ELIGIBILITY AND TECHNICAL CRITERIA:

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

7. 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.

8. 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.

9. 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.

10. EARNEST MONEY DEPOSIT (EMD): Not applicable

11. BID PREPARATION AND SUBMISSION:

The Bid is to be submitted separately for technical and Price on portal of e-Procurement agency for

- i. Engaging CAT-I Competent ISSPs from GITC empanelled vendors and ISD empanelled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department in response to the RFP No. SBI/GITC/ISD/2024-25/ISO/27(RFP-1426) **Dated 07.02.2025.** 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 EMD and Tender Fee as specified in this document.

Or

Proof of remittance of EMD (if directly credited in designated account) and Tender Fee as specified in this document. In case, EMD is submitted in form of BG, scanned copy of original BG should be uploaded subject to compliance of requirement mentioned in clause no 11 “*DEADLINE FOR SUBMISSION OF BIDS*” sub-clause (ii).

- (d) Specific response with supporting documents in respect of Eligibility Criteria as mentioned in **Appendix-B** 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“*DEADLINE FOR SUBMISSION OF BIDS*” sub-clause (ii).

- (i) If applicable, copy of registration certificate issued by competent authority as mentioned in SI No 2 of Eligibility Criteria under Appendix-B.
- ii. Indicative Price Bid for Engaging CAT-I Competent ISSPs from GITC empanelled vendors and ISD empanelled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT-NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT-AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department in response to the RFP No. SBI/GITC/ISD/2024-25/ISO/27(RFP-1426) **Dated 07.02.2025** . 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 provide.
- (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. 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.

12. 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 SI 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 upto 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.

13. 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 the forfeiture of EMD submitted by the Bidder.

14. 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 Bank will not forfeit its EMD. 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.

15. 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.

16. 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, EMD and 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.

17. 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.

18. 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.

19. 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.

1. 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 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 self-certification as per **Appendix-G** that the product or service offered meets the minimum local content requirement for ‘Class-I local supplier’/ ‘Class-II local supplier’ as the case may be and shall give details of location(s) at which the local value addition is made.

- 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 EMD and/or 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. The EMD of each unsuccessful Bidder will be discharged and returned.

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. SERVICES:

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

- iii. Service Provider support staff should be well trained to effectively handle queries raised by the customers/employees of the Bank.
- iv. Updated escalation matrix shall be made available to the Bank once in each quarter and each time the matrix gets changed.

26. PENALTIES:

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

27. 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.

28. 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 authority(ies). 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.).
- iv. Service provider shall grants unrestricted and effective access to a) data related to the outsourced activities; b) the relevant business premises of the service provider; subject to appropriate security protocols, for the purpose of effective oversight use by the Bank, their auditors, regulators and other relevant Competent Authorities, as authorised under law.

29. SUBCONTRACTING:

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

30. VALIDITY OF AGREEMENT:

The Agreement/ SLA will be valid for the period of job completion. The Bank reserves the right to terminate the Agreement as per the terms of RFP/ Agreement.

31. LIMITATION OF LIABILITY:

- i. The maximum aggregate liability of Service Provider, subject to below mentioned sub-clause (*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 abovementioned sub-clause (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.

32. CONFIDENTIALITY:

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

33. 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, it’s 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).

34. 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. Service Provider shall report the incidents, including cyber incidents and those resulting in disruption of service and data loss/ leakage immediately but not later than one hour of detection.
- vii. The Service Provider shall execute Data Processing Agreement on the format attached as Appendix-P to this RFP.

- viii. Service Provider shall abide by the provisions of the DPDP Act, 2023 - 11th August, 2023; CG-DL-E-12082023-248045 as and when the relevant rules and guidelines come into force.

35. 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, data flow documents, data register and data dictionary 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.**

36. INTELLECTUAL PROPERTY RIGHTS AND OWNERSHIP:

- i. For any technology / software / product used/supplied 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 below mentioned sub-clause (iv) and (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 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.
- 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. 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 RFP shall be deemed to be 'work made for hire' under any Indian/U.S. or any other applicable copyright laws.
- vii. The Intellectual Property Rights on the software code, copyright and source code for various applications/ interfaces developed under this RFP, and any other component/ framework/ middleware used/ developed as pre-built software assets to deliver the solution, shall belong to the Bank and the Bank shall have complete and unrestricted rights on such property. However, Service Provider shall hold All Intellectual Property rights in any pre-built software *per se*, except for those which have been assigned under this RFP.
- viii. All information processed by Service provider during software maintenance 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.

37. 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 3% of total Project Cost for delay of each week or part thereof maximum up to 15% of total Project Cost. Once the maximum deduction is reached, the Bank may consider termination of the Agreement.

| S.No | Description | Liquidated Damages/LD* |
|------|---|--|
| 1 | Service Provider shall provide acknowledgement within 2 Working Days from receipt of PO | Rs. 100,000 per day for delay in providing acknowledgement subject to maximum up to Rs. 5,00,000. |
| 2 | Service Provider shall provide PO acceptance within 3 Working Days from date of acknowledgement of PO. | Rs. 100,000 per day for delay in providing acceptance subject to maximum up to Rs. 5,00,000. |
| 3 | Service Provider shall provide detailed CVs specifying the professional experience of minimum 120% of the number of resources required per category as per the PO within 1 Working Days from the date of acceptance of PO or within 1 days for submission of additional CVs as mentioned in para (a) of Delivery schedule and Scope of work | 0.35% of the yearly PO value corresponding to the pending resumes per day subject to maximum up to 1.75% of the yearly PO value corresponding to the pending resumes. |
| 4 | The resources have to report within 3 days from the date of finalization of the resources by the Bank or a later period that may be specified in the PO. | 0.50% of the yearly PO value corresponding to the pending resources to be onboarded per day subject to maximum up to 3% of the yearly PO value of the resources pending to be onboarded. |
| 5 | Provision of CVs and onboarding of substitute resources as specified in Clauses (j) as defined in this annexure | The Liquidated Damages as mentioned in S. No 3 and 4 mentioned above will apply. |

38. 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.

39. 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 a 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 upto 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 empaneled 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 " *CODE OF INTEGRITY AND DEBARMENT/BANNING* " sub-clause (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 EOIRFP 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 has 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.

40. 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 abovementioned sub-clause (i) (a) to (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 20% 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.

41. FORCE MAJEURE:

- i. Notwithstanding the provisions of terms and conditions contained in this RFP, 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.
- 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.

42. 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.

43. 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.

44. 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.

45. GOVERNING LANGUAGE:

The governing language shall be English.

46. 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.

47. 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 GST. All other present and future tax /duties, if any applicable and also cost of incidental services such as transportation, road permits, insurance etc. should be included in the price quoted.. 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. Parties shall fulfil all their respective compliance requirements under the GST law. This shall include (but not be limited to):
 - (a) Bank shall pay GST amount after verifying the details of invoice on GSTR 2B on GSTN portal.
 - (b) In case any credit, refund or other benefit is denied or delayed to the Bank due to any non-compliance of GST Laws by the vendor including but not limited to, failure to upload the details of invoice or any other details of the supply of goods or services, as the case may be, as required under GST Law on the appropriate government's goods and services tax network portal, the failure to pay applicable GST to the Government or due to non-furnishing or furnishing of incorrect or incomplete documents by the party, vendor would reimburse the loss to the Bank including, but not limited to, any tax loss or denial of credit, interest and penalty and reasonable fee for contesting the demand. Amount payable under this clause shall survive irrespective of termination of agreement if the demand pertains to the agreement period.
 - (c) In case of any tax demand or denial of ITC or refund or any other benefit by the GST authorities, both the parties may mutually decide whether to contest the matter. In case, it is decided to contest the matter, the vendor is required to deposit the disputed demand including interest and penalty proposed with the other party without waiting for the outcome of the legal proceeding. In case the matter is finally decided in favour of the other party, the other party is required to refund the amount received from the defaulting party without any interest.
- vii. 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.

48. 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.
- iii. Bank will deduct TDS at applicable rate while making payment under GST Act 2017 and Income Tax Act 1961.

49. TENDER FEE: Not applicable

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.

50. EXEMPTION OF EMD AND TENDER FEE:

Micro & Small Enterprises (MSE) units and Start-ups* are exempted from payment of EMD 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 EMD/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 EMD/ 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 /EMD will be summarily rejected and no queries will be entertained.

51.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 (ISO)
State Bank of India
Information Security Department,
State Bank Global IT Centre,
Ground Floor, A Wing, Sector 11,
CBD Belapur, Navi Mumbai-400614

Dear Sir,

Ref: RFP No. SBI/GITC/ISD/2024-25/ISO/27 dated 07.02.2025

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

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, organisation 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 we (participating in RFP as OEM)/ our OEM have a support center and level 3 escalation (highest) located in India.
- xv. 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.
- xvi. 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 along with subsequent Orders and its amendment thereto 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 (where applicable evidence of valid certificate to be attached). We certify that we and our OEM fulfil all the requirements in this regard and are eligible to participate in this RFP.

- xvii. 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.
- 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 20..

(Signature)

(Name)

(In the capacity of)

Duly authorised to sign Bid for and on behalf of

Seal of the company.

Appendix-B

Technical – Evaluation Parameter

| SL No. | Activities related to Information Security | Yes / No | Details required in Annexure as per C1 to C4 |
|---------------|--|-----------------|---|
| 1 | Indian/Global BFSI 3 distinct clients' assignments handled in Information /Cyber security (In Public Sector Bank(/ Private Sector Bank / Global Bank during the last five years(FY-2019-2024).Among these 3 distinct clients minimum 2 clients should be from Indian Public sector/Private Bank. Public Sector Bank / Private Sector Bank / Global Bank -The Banks should have more than 250 branches. Please Note: Supporting Documents-Purchase order/Work Order/Client Reference to be furnished | Yes / No | C1 |
| 2 | Engagement of the organisation in the industry for last 10years. | Yes / No | C2 |
| 3 | Credentials / certifications of CERT-In | Yes / No | C3 |
| 4 | Minimum 2 engagements of the organization in the BFSI sector in context of scope of work – Security review during last three FYs (FY-2021-2024). (Supporting Documents-Purchase order/Work Order/Client Reference to be furnished) | Yes / No | C4 |

Technical Evaluation Excel sheet has also been shared along with this RFP for the information of the bidders. Bidders should fill in their credentials in the Technical evaluation sheet and share with the Bank as a part of technical bid. Bidders to note

that, eligibility will be based on the credentials filled in by the bidders shall not be final and binding on the Bank. The Bank's decision on shortlisting of bidders as a part of technical evaluation thereof shall be final. Bidders will be shortlisted on the basis of fulfilment of all the criteria as desired by the Bank based on technical evaluation

Post engagement, the allocation / distribution of activities / assignments will be solely at the discretion of the Bank. The Bank will assign the services to the authorised person of the successful bidders who will manage the whole. The Bank reserves the right to accept the bids or opt for negotiation and offer the rates or cancel the entire RFP process.

Bidders will be shortlisted on the basis of fulfilment of all the criteria desired by the Bank based on technical evaluation and presentation (if required) at the discretion of the Bank

Bidders found unqualified will not be considered for further evaluation/reverse auction.

However, Bank reserves right to evaluate periodically i.e. Monthly/quarterly/Yearly.

Bidders to provide required details as per Annexure C1 to C4 for Sl.No.1 to 4 above.

******The bidders to furnish each document in chronological order. Name and section duly mentioned at the top of each document.**

Signature and Seal of Company

Annexure C1

Assignments handled by the organization

(Assignments handled of minimum 3 distinct clients under Information / Cyber security domain (In Public Sector Bank / Private Sector Bank / Global Bank) during the last five years(FY-2019-2024).) Among these 3 distinct clients minimum 2 clients should be from Indian Public sector/Private Bank.

A1. Assignments:

| <u>Sl No.</u> | <u>Assignments handled (Last 5 years)- FY 2019-2020,2020-21,2021-22 ,2022-23 and 2023-24</u> | <u>Name of the Client</u> | <u>Nature of work/Job allocated</u> | <u>Date of the Purchase order/work order</u> |
|---------------|--|---------------------------|-------------------------------------|--|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |

Please Note:

- Supporting documents for above should be Purchase / Work Orders, letters from clients on their letter head, contacts of clients etc.

Public Sector Bank / Private Sector Bank / Global Bank -The Banks should have more than 250 branches.

Signature

Seal of Company

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

Annexure C2

Engagement of organization in the Industry

| <u>Sl No.</u> | <u>Name of the Organization</u> | <u>Date of Incorporation</u> | <u>Number of years of engagement in the Industry</u> |
|---------------|---------------------------------|------------------------------|--|
| 1 | | | |
| 2 | | | |
| 3 | | | |

Signature

Seal of Company

Please Note:

- Certificate of Incorporation and KYC of the Organisation

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

Annexure C3

CERT-In Certification

| SI No. | CERT-In Certification | Date of Issuance | Enclosed(Yes/No) |
|--------|-----------------------|------------------|------------------|
| 1 | | | |

Signature

Seal of Company

Please Note:

- Supporting documents for above should be nominations/certifications/documents etc.

Annexure C4

Engagement of the organisation in the BFSI sector in context with the scope of work –Security Review

For the period April 2021 to March 2024

| Sl.No. | Name of the organisation where engaged | Nature of work(Detailed Description) | Date of Purchase order (2020-23) | Supporting documents (Enclosed /Not Enclosed) |
|--------|--|--------------------------------------|----------------------------------|---|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |

Please Note:

- Supporting documents for above should be Purchase / Work Orders, letters from clients on their letter head, contacts of clients etc.

Signature

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 authorised signatory

Seal of Company

Appendix-E

Scope of Work and Payment Schedule

Comprehensive Security Review (CSR) of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

Scope:

Details of Applications as per Appendix- E.

The Major Scope of the Security review of Applications as per Appendix-E is summarized below:

a) Secure Network Architecture Review

Not applicable

b) Application security review

- b.1 AppSec of application
- b.2 Role based Application review
- b.3 Application threat modelling
- b.4 Cloud security review(if applicable)

c) VA/PT of all the Assets in scope

Not applicable

4 Configuration Audit

- 4.1. Configurations of All components such as OS, Database, Application server, web server etc. need to be reviewed (script based or manual) against Bank's Benchmark Document.

5 Process Review: Process flow including.

- 5.1. User management, privilege access etc., change control management, generation and checking of logs, incident management, flow of both to & fro traffic (its contents and the format in which it is travelling), storage at

any point, password management, security environment, Compliance with RBI and local regulatory guidelines and Local Privacy Law and Bank's IT Policy and IS Policy and industry best practices.

- 5.2. Assessment of security risk involved in data being processed/handled at third party vendor's site/location covering end to end data flow to ensure CIA of information.
- 5.3. Review of each Database-on-database security perspective.
- 5.4. Review of Vendor/ Third Party Access management
- 5.5. In view of a few Applications under scope are with third party vendors, the selected ISSP must review the controls implemented by the vendor for Bank's Data processing as against Bank's set in controls at third party data processing of Bank's data.
- 5.6. Data Flow Diagram for all the Applications to be obtained and 'end to end' process review, specifically on third party locations, if any need to be carried out.

6 Source code review – Source code review wherever applicable as per the Appendix E(Code Deployment Process)

7 API Review: API review as per Appendix E.

8 Assessment of Forensic readiness and threat intelligence for individual Applications.

9 Preparedness for Ransomware:

Not applicable

10 Data Security

- a) Assessment of Backup process
- b) Evaluation of enforcement of the defined back up process and Restoration testing.
- C) Compliance on patch management.

11 Compliance Review – as per Bank's IT & IS Policy, Cyber Security Policy, RBI Guidelines and Best Global Security practices.

12 Confirmatory Review: If 100% compliance is not achieved in first round, the ISSP must do subsequent confirmatory reviews till the 100% closure of the observations. However, the 100% payment will be released after first round of confirmatory review on the condition of submitting an undertaking by the ISSP that, they will do the subsequent confirmatory review as a part of the assignment without any additional cost to the bank.

2. Deliverable for the Engagement:

- a) Hash Value and version number of every application (as advised by the Application Owner and for which it was reviewed) will be required to be incorporated in the final report for both initial and confirmatory review.
- b) Detailed Report highlighting vulnerabilities in the system. Technical vulnerability identified should provide: Risk impact (High, Medium, Low), possibility of occurrence (High/Medium/Low), ease of exploitation (Easy/Difficult/Very Difficult), specific mitigation measures keeping in view the criticality of the application, placement of the systems, type of the information passing over the channel, compensatory controls etc. If the service is vulnerable, screen shot/logs depicting vulnerability and change required in Secured Configuration Document may also be suggested.
- c) If any observation has been made which is as per the global best practices and not included in the Bank's latest policies, RBI guidelines and IT Act, the relevant reference will have to be provided in the report by the ISSP.
- d) Both initial and final reports (after completion of the confirmatory review) will have to be presented application wise.
- e) A summary report (component wise) for all the applications/review areas (combined) will also be a part of both the reports.
- f) Both safe as well as unsafe findings are required to be listed along with the Mitigation tracker, listing the unsafe findings.
- g) An application and activity wise daily tracker to be provided to the Application Owner and Information Security Department.
- h) Recommendations for risk containment based on global best practices, Compliance to the latest SBI IT Policy, Information Security Policy, RBI guidelines, Local Regulatory Guidelines and IT Act 2008 etc. requirements would be required to be evaluated and reported.
- i) 100% confirmatory review will be required to be conducted. However, if the 100% confirmatory is not covered in first round, the Bank reserves the right to call the ISSP team to conduct other round(s) of confirmatory test, under prior intimation, if required, without any extra cost.
- j) Along with the soft copy of the final report, its printout with all pages signed by the authorized signatory under your company's seal must be submitted. The complete report should contain the following information also: -

Date of report

- o Exact period of conduct of the review and/or confirmatory review (as the case may be)

- Running page number for all pages
 - Name and designation of the officials from Application Owner department with whom the findings had been discussed and finalized.
- k) If the ISSP resource is required to visit Bank’s vendor partner’s premises and/or for conducting White Box testing of the Source Code, the NDA will be signed between the ISSP resource and the Bank’s vendor partner invariably.
- l) E-Mail response from the Application Owner team may suffice in most of the cases of any reference in respect of the observations made. However, if required, the ISSP resource will be required to visit SBI for a one-on-one interaction on one or more instances with the Application Owner and/or Information Security Department.
- m) ISSP to suggest risk containment / risk mitigation controls in case some of the remediation suggested in the report cannot be implemented because of technical or business-related reasons-application dependency.
- n) **Delivery Schedule:** The initial review is to be completed and report to be submitted within 3 months from the date of Purchase Order. In case, after selection of L-1 ISSP, there is a delay in placing the formal Purchase Order, the Bank may provide a mail confirmation that the ISSP has been selected by the Bank for conducting the captioned review and the review process may be started on a notice of one day (formal Purchase Order may be placed by the Bank later).
- o) All the payments shall be made by the Bank to the Selected Bidder except as otherwise provided in the bid after deducting all taxes including TDS, as per laid down provisions from time to time. All the payment shall be in Indian Rupees. The detailed payment terms are given below: -

| S.No. | Description | Terms of Payment |
|-------|--|------------------|
| 1 | After submission of Reports of 1 st Round of Review | 70% |
| 2 | After submission of Reports of Confirmatory Review | 30% |

- a. Adequate number of resources should be deployed for assigned CSR activities within 7 days of issuance of PO date.
- b. The initial review of assigned CSR activity must be completed within three months of the kick-off meeting date.

DEPLOYMENT OF RESOURCES:

The bidders should deploy sufficient resources for review activities as per Skill-set and educational/professional criteria of this RFP within 7 days from the date of Purchase order. The detailed profile of the resources is to be uploaded in the e-tender portal .The defined resources may be interviewed to meet our desired requirements. If any resource is found unsuitable during the deployed period, the successful bidder has to provide an immediate replacement within 2 working days from the date of intimation. In case of resource resignation/termination during the deployed period, the successful bidder has to make necessary arrangement and provide an immediate alternative/replacement. In case the bidder fails to deploy as above, entire contract/assignment will be cancelled, and the penalty will be levied.

Deliverable for the Engagement:

- p) Hash Value and version number of every application (as advised by the Application Owner and for which it was reviewed) will be required to be incorporated in the final report for both initial and confirmatory review.
- q) Detailed Report highlighting vulnerabilities in the system. Technical vulnerability identified should provide: Risk impact (High, Medium, Low), possibility of occurrence (High/Medium/Low), ease of exploitation (Easy/Difficult/Very Difficult), specific mitigation measures keeping in view the criticality of the application, placement of the systems, type of the information passing over the channel, compensatory controls etc. If the service is vulnerable, screen shot/logs depicting vulnerability and change required in Secured Configuration Document may also be suggested.
- r) If any observation has been made which is as per the global best practices and not included in the Bank's latest policies, RBI guidelines and IT Act, the relevant reference will have to be provided in the report by the ISSP.
- s) Both initial and final reports (after completion of the confirmatory review) will have to be presented application wise.
- t) A summary report (component wise) for all the applications/review areas (combined) will also be a part of both the reports.
- u) Both safe as well as unsafe findings are required to be listed along with the Mitigation tracker, listing the unsafe findings.
- v) An application and activity wise daily tracker to be provided to the Application Owner and Information Security Department.
- w) Recommendations for risk containment based on global best practices, Compliance to the latest SBI IT Policy, Information Security Policy, RBI guidelines, Local Regulatory Guidelines and IT Act 2008 etc. requirements would be required to be evaluated and reported.
- x) 100% confirmatory review will be required to be conducted. However, if the 100% confirmatory is not covered in first round, the Bank reserves the right to call the ISSP team to conduct other round(s) of confirmatory test, under prior intimation, if required, without any extra cost.

- y) Along with the soft copy of the final report, its printout with all pages signed by the authorized signatory under your company's seal must be submitted. The complete report should contain the following information also: -
- Date of report
- Exact period of conduct of the review and/or confirmatory review (as the case may be)
 - Running page number for all pages
 - Name and designation of the officials from Application Owner department with whom the findings had been discussed and finalized.
- z) If the ISSP resource is required to visit Bank's vendor partner's premises and/or for conducting White Box testing of the Source Code, the NDA will be signed between the ISSP resource and the Bank's vendor partner invariably.
- aa) E-Mail response from the Application Owner team may suffice in most of the cases of any reference in respect of the observations made. However, if required, the ISSP resource will be required to visit SBI for a one-on-one interaction on one or more instances with the Application Owner and/or Information Security Department.
- bb) ISSP to suggest risk containment / risk mitigation controls in case some of the remediation suggested in the report cannot be implemented because of technical or business-related reasons-application dependency.

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

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.

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

| Sl. No. | Project Details | Total Cost |
|---------|---|------------|
| 1 | Indicative Commercial Bid for Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review (CSR) of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT-TRADE FINANCE (FY 2024-25) Department | |
| | Total | |

(Amount quoted in INR exclusive of GST/CGST)

Dated this day of 2025

(Signature)

(Name)

(In the capacity of)

Duly authorized to sign Bid for and on behalf of

Seal of the company.

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.>

OR

Format for Self-Certification of Local Content

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.

1. The details of location(s) at which the local value addition is made are as under:

| SI No | Product details | Name of place |
|-------|-----------------|---------------|
| 1 | | |
| 2 | | |

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

Signature of authorised official

Name:

Company seal:

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:xx:xx dated dd/mm/yyyy.
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

Other terms and Penalties

i.If existing Service Provider is breach of obligation mentioned in the RFP, they shall be liable for paying a penalty to an extent of 20% 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.

ii.Adequate number of resources should be deployed for assigned CSR activities within 7 days of issuance of PO date.

iii.The initial review of assigned CSR activity must be completed within three months of the kick-off meeting date.

Condition 1 Below penalty clause will be applicable if:

| Sl. No | TAT for initial review | Penalty |
|--------|---|------------------------|
| 1 | Kick Off meeting should be initiated within 10 working days of issuance of P.O. date. | Rs. 5000/- per week ** |
| 2 | If CSR initial review is not initiated within 7 Days of kick off meeting Date | Rs. 1000/- per week ** |
| 3 | Completion of initial CSR review beyond 3 months of kick off meeting. | Rs. 1000/- per week ** |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

****The above-mentioned penalty will be only applicable if the delay is on part of ISSP.**

Condition 2: If bidders fail to provide the confirmatory review within the defined TAT of three months after completion of initial review

| <u>S. No</u> | <u>TAT for initial review</u> | <u>Penalty</u> |
|--------------|-------------------------------|-------------------------------|
| <u>1</u> | <u>Beyond 4 months</u> | <u>Rs. 1000/- per week **</u> |

****The above-mentioned penalty will be only applicable if the delay is on part of ISSP.**

The maximum penalty due to non-adherence of SLA will not exceed 20% of bill amount payable to the vendors.

****The above-mentioned penalty will be only applicable if the delay is on part of ISSP.**

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

Appendix–J

Service Level Agreement

AGREEMENT FOR ENGAGING CAT-I COMPETENT ISSPS FROM GITC EMPANELED VENDORS AND ISD EMPANELED VENDORS FOR COMPREHENSIVE SECURITY REVIEW (CSR) OF APPLICATIONS OF IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) DEPARTMENT

**STATE BANK OF INDIA,
Information Security Department
'A'- Wing, Ground Floor
Sector 11, CBD Belapur
Navi Mumbai 400614
INDIA**

AND

1

Date of Commencement : _____ 2

Date of Expiry : _____

1 The other Party (Contractor/ Service Provider) to the Agreement

2 Effective Date from which the Agreement will be operative.

Contents

| | | |
|-----|--|----|
| 1. | SCHEDULE OF EVENTS | 2 |
| 2. | INVITATION TO BID:..... | 6 |
| 3. | DISCLAIMER: | 7 |
| 4. | DEFINITIONS:..... | 8 |
| 5. | SCOPE OF WORK: | 9 |
| 6. | ELIGIBILITY AND TECHNICAL CRITERIA: | 9 |
| 7. | COST OF BID DOCUMENT:..... | 9 |
| 8. | CLARIFICATION AND AMENDMENTS ON RFP/PRE-BID MEETING: | 9 |
| 9. | CONTENTS OF BID DOCUMENT:..... | 10 |
| 10. | EARNEST MONEY DEPOSIT (EMD):..... | 10 |
| 11. | BID PREPARATION AND SUBMISSION: | 11 |
| 12. | DEADLINE FOR SUBMISSION OF BIDS: | 13 |
| 13. | MODIFICATION AND WITHDRAWAL OF BIDS:..... | 13 |
| 14. | PERIOD OF BID VALIDITY AND VALIDITY OF PRICE QUOTED IN REVERSE AUCTION (RA): | 14 |
| 15. | BID INTEGRITY:..... | 14 |
| 16. | BIDDING PROCESS/OPENING OF TECHNICAL BIDS: | 14 |
| 17. | TECHNICAL EVALUATION: | 15 |
| 18. | EVALUATION OF INDICATIVE PRICE BIDS AND FINALIZATION: | 16 |
| 19. | CONTACTING THE BANK: | 17 |
| 20. | POWERS TO VARY OR OMIT WORK: | 20 |
| 21. | WAIVER OF RIGHTS:..... | 20 |
| 22. | CONTRACT AMENDMENT: | 21 |
| 23. | BANK’S RIGHT TO ACCEPT ANY BID AND TO REJECT ANY OR ALL BIDS: | 21 |
| 24. | BANK GUARANTEE: | 21 |
| 25. | SERVICES:..... | 21 |
| 26. | PENALTIES: | 22 |
| 27. | RIGHT TO VERIFICATION:..... | 22 |
| 28. | RIGHT TO AUDIT: | 22 |
| 29. | SUBCONTRACTING: | 23 |
| 30. | VALIDITY OF AGREEMENT: | 23 |
| 31. | LIMITATION OF LIABILITY:..... | 23 |
| 32. | CONFIDENTIALITY:..... | 24 |
| 33. | DELAY IN SERVICE PROVIDER’S PERFORMANCE: | 24 |
| 34. | SERVICE PROVIDER’S OBLIGATIONS: | 25 |
| 35. | TECHNICAL DOCUMENTATION: | 26 |
| 36. | INTELLECTUAL PROPERTY RIGHTS AND OWNERSHIP: | 26 |
| 37. | LIQUIDATED DAMAGES:..... | 28 |
| 38. | CONFLICT OF INTEREST:..... | 28 |
| 39. | CODE OF INTEGRITY AND DEBARMENT/BANNING:..... | 30 |
| 40. | TERMINATION FOR DEFAULT: | 33 |
| 41. | FORCE MAJEURE:..... | 35 |
| 42. | TERMINATION FOR INSOLVENCY: | 36 |
| 43. | TERMINATION FOR CONVENIENCE: | 36 |
| 44. | DISPUTES / ARBITRATION (APPLICABLE IN CASE OF SUCCESSFUL BIDDER ONLY): | 36 |
| 45. | GOVERNING LANGUAGE: | 37 |
| 46. | APPLICABLE LAW:..... | 37 |
| 47. | TAXES AND DUTIES: | 37 |
| 48. | TAX DEDUCTION AT SOURCE:..... | 39 |
| 49. | TENDER FEE: | 39 |
| 50. | EXEMPTION OF EMD AND TENDER FEE: | 39 |

| | |
|---|-------------------------------------|
| 51. NOTICES:..... | 40 |
| APPENDIX –A | 41 |
| APPENDIX-B | 45 |
| APPENDIX-C..... | ERROR! BOOKMARK NOT DEFINED. |
| ANNEXURE C4 | 50 |
| APPENDIX-D..... | 51 |
| APPENDIX-E | 52 |
| APPENDIX-F | 58 |
| APPENDIX–G | 60 |
| APPENDIX–H..... | 62 |
| APPENDIX–I | 65 |
| APPENDIX–J | 67 |
| 1. DEFINITIONS & INTERPRETATION | 71 |
| 2. SCOPE OF WORK | 74 |
| 3. FEES /COMPENSATION | 74 |
| 4. LIABILITIES/OBLIGATION | 77 |
| 5. REPRESENTATIONS &WARRANTIES | 79 |
| 6. GENERAL INDEMNITY | 81 |
| 7. CONTINGENCY PLANS..... | 81 |
| 8. TRANSITION REQUIREMENT..... | 82 |
| 9. LIQUIDATED DAMAGES | 82 |
| 10. RELATIONSHIP BETWEEN THE PARTIES | 83 |
| 11. SUB CONTRACTING | 84 |
| 12. INTELLECTUAL PROPERTY RIGHTS | 84 |
| 13. INSPECTION AND AUDIT | 85 |
| 14. CONFIDENTIALITY | 87 |
| 16. TERMINATION..... | 90 |
| 17. DISPUTE REDRESSAL MACHANISM & GOVERNING LAW..... | 92 |
| 19. WAIVER OF RIGHTS | 93 |
| 20. LIMITATION OF LIABILITY | 94 |
| 21. FORCE MAJEURE..... | 95 |
| 22. NOTICES | 96 |
| 23. GENERAL TERMS & CONDITIONS..... | 97 |
| ANNEXURE-A | 100 |
| ANNEXURE-B..... | 104 |
| ANNEXURE-C | ERROR! BOOKMARK NOT DEFINED. |
| ANNEXURE-D | ERROR! BOOKMARK NOT DEFINED. |
| ANNEXURE-E..... | ERROR! BOOKMARK NOT DEFINED. |
| ANNEXURE-F | ERROR! BOOKMARK NOT DEFINED. |
| ANNEXURE-G | 113 |

| | |
|------------------|-------------------------------------|
| APPENDIX–K..... | 129 |
| APPENDIX–L | 135 |
| APPENDIX–M | 136 |
| APPENDIX–N..... | ERROR! BOOKMARK NOT DEFINED. |
| APPENDIX–O..... | ERROR! BOOKMARK NOT DEFINED. |

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 Information Security Department,³ 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

_____ ⁴ 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

- (i) “The Bank” is carrying on business in banking in India and overseas and desirous to avail services for Engaging competent forty-one (41) resources on Application Managed Services to work in bank environment for a period of one year- Project-II-August2024Service Provider is in the business of providing _____ and has agreed to provide the services as may be

³Name & Complete Address of the Dept.

⁴Name & Complete Address (REGISTERED OFFICE) of service Provider,

required by the Bank mentioned in the Request of Proposal (RFP) No SBI/GITC/ISD/2024-25/ISO/27 (RFP-1426) dated 07.02.2025 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 (name of the Software/ Hardware/ Maintenance Services) ~~<Strike off whichever is inapplicable>~~,⁵ such that any reader of the Documentation can access, use and maintain all of the functionalities of the (Service)⁶, without the need for any further instructions. ‘Documentation’ includes, user manuals, installation manuals, operation manuals, design documents, process documents, data flow documents, data register, technical manuals, functional specification, software requirement specification, on-line tutorials/CBTs, system configuration documents, Data Dictionary, 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.

⁵ Name of Software/ Maintenance services

⁶ Name of Software

1.1.7 “Request for Proposal (RFP)” shall mean RFP NO. SBI/GITC/ISD/2024-25/ISO/27 (RFP-1426) dated 07.02.2025. 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.

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 **Appendix-E**

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.

3.2 All duties and taxes (excluding GST,CGST or other Local taxes 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

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

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 schedule⁷ specified in this Agreement.

⁷ Please ensure that the time scheduled is suitably incorporated in the Agreement.

3.5.5 Service Provider shall be liable to pay penalty at the rate mentioned in **Appendix-I** 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

4.2 The Bank shall provide necessary support to Service Provider/ Vendor in the performance of the Services, including, providing reasonable facilities and timely access to data, information and personnel of the Bank.**Service Provider Duties**

(i) Service Delivery responsibilities

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

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

(c) 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.

(d) Service Provider agrees and declares that it shall be the sole responsibility of Service Provider to comply with the provisions of all the applicable laws, concerning or in relation to rendering of Services by Service Provider as envisaged under this Agreement.

- (e) Service Provider shall be responsible to provide Data Dictionary in a format provided by the Bank. During the term of this Agreement, such a format may be revised by the Bank as per the requirements. Service Provider shall capture all the fields in Data Dictionary format and keep the same always updated during the term of this Agreement.
- (f) Service Provider shall report the incidents, including cyber incidents and those resulting in disruption of service and data loss/ leakage immediately but not later than one hour of detection.
- (g) The Service Provider shall execute Data Processing Agreement on the format attached as Appendix-G to this RFP. < This term is applicable where the activities for which selection of Vendor/ outsourcing of activities involve access/sharing/transfer of Personal Data/PII of EU/UK NRI customers. STRIKE OFF, IF NOT APPLICABLE.>
- (h) Service Provider/ Vendor shall abide by the provisions of the DPDP Act, 2023 - 11th August, 2023; CG-DL-E-12082023-248045 as and when the relevant rules and guidelines come into force.
- (i) The selected vendor must submit the Profile, KYC, Police verification, educational qualification and experience of the resources going to be deputed for the assignment to the ISD . The ISD team’s discretion is final in accepting the resources for the project
- (j) The resources deployed for the purpose must sign the non-disclosure agreement as per the IS Policy of the Bank, wherever required.
- (k) Selected vendor shall deploy the resources to start the activity at our mail/telephonic confirmation that they have been selected to take-up the job pending formal purchase order on 2 days’ notice.
 - i. The resources has to be deployed on-site at SBI ,GITC ,Navi Mumbai, Belapur.
 - ii. The Security review will be carried out from Bank’s GITC, Belapur office and for outstation Application review (outside Mumbai), the out-of-pocket expenses and economy air fare will be reimbursed as per the Service Level Agreement to be signed with the ISSPs.

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 and products 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 at the time of delivery the software deployed/ upgraded 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 delivered as well as any subsequent versions/modifications done). Software deployed/ upgraded 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, provident 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 During the Contract period, if any software or any component thereof is supplied by Service Provider is inoperable or suffers degraded performance, Service provider shall, at the Bank's request, promptly replace the software or specified component with new software of the same type and quality. Such replacement shall be accomplished without any adverse impact on the Bank's operations within agreed time frame and without any additional cost to the Bank.

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 software/ hardware/ 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

Service Provider shall arrange and ensure proper data recovery mechanism, attrition plan and other contingency plans to meet any unexpected obstruction to 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.

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 vendor is found to be in breach of this obligation, they shall be liable for paying a penalty as defined in the **RFP No. SBI/GITC/ISD/2024-25/ISO/27(RFP-1426) dated 07.02.2025** 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 Appendix I.

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 0.5% of total Project

cost for delay of each week or part thereof maximum up to 20% of total Project cost. Once the maximum deduction is reached, the Bank may consider termination of agreement.

| S.No | Description | Liquidated Damages/LD* |
|------|---|--|
| 1 | Service Provider shall provide acknowledgement within 2 Working Days from receipt of PO | Rs. 1,000 per day for delay in providing acknowledgement subject to maximum up to Rs. 1,00,000. |
| 2 | Service Provider shall provide PO acceptance within 5 Working Days from date of acknowledgement of PO. | Rs. 2,000 per day for delay in providing acceptance subject to maximum up to Rs. 1,00,000. |
| 3 | Service Provider shall provide detailed CVs specifying the professional experience of minimum 120% of the number of resources required per category as per the PO within 14 Working Days from the date of acceptance of PO or within 7 days for submission of additional CVs as mentioned in para (a) of Delivery schedule and Scope of work. | 0.35% of the yearly PO value corresponding to the pending resumes per day subject to maximum up to 1.75% of the yearly PO value corresponding to the pending resumes. |
| 4 | The resources have to report within 35 days from the date of finalization of the resources by the Bank or a later period that may be specified in the PO. | 0.50% of the yearly PO value corresponding to the pending resources to be onboarded per day subject to maximum up to 3% of the yearly PO value of the resources pending to be onboarded. |
| 5 | Provision of CVs and onboarding of substitute resources as specified in Clauses (j) as defined in this annexure | The Liquidated Damages as mentioned in S. No 3 and 4 mentioned above will apply. |

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/supplied 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 below mentioned sub-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.).
- 13.4 Service Provider shall grants unrestricted and effective access to a) data related to the Services; b) the relevant business premises of the Service Provider; subject to appropriate security protocols, for the purpose of effective oversight use by the

Bank, their auditors, regulators and other relevant Competent Authorities, as authorised under law.

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 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.
- 14.10 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.
- 14.11 Upon expiration or termination of the Agreement, all the Bank's proprietary documents, customized programs partially or wholly completed and associated documentation, or the Bank's materials which are directly related to any project under the Agreement shall be delivered to the Bank or at the Bank's written instruction destroyed, and no copies shall be retained by Service provider without the Bank's written consent.
- 14.12 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 The Intellectual Property Rights on the software code, copyright and source code for various applications/ interfaces developed under this Agreement, and any other component/ framework/ middleware used/ developed as pre-built software assets to deliver the solution, shall belong to the Bank and the Bank shall have complete and unrestricted rights on such property. However, Service Provider shall hold All Intellectual Property rights in any pre-built software *per se*, except for those which have been assigned under this Agreement.
- 15.3 All information processed by Service Provider during software maintenance 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 above mentioned sub-clause (i) to (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 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, if any, or in discharge of any obligation arising out of this Agreement and 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 the dispute occurs, as evidenced through the first written communication from any Party notifying the other regarding the disputes, the same shall be referred to and be subject to the jurisdiction of competent Civil Courts of Mumbai only. The Civil Courts in Mumbai, Maharashtra shall have exclusive jurisdiction in this regard.
- 17.2 Service Provider shall continue work under the Contract during the dispute resolution 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 competent court is obtained.
- 17.3 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 below mentioned sub-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 above mentioned sub-Clause 20.1 shall not apply with respect to:

- (i) claims that are the subject of indemnification pursuant to Clause 12⁸ (infringement of third party Intellectual Property Right);
- (ii) damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider;
- (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 above mentioned sub-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

⁸ Please see Clause 12 ‘IPR Indemnification’

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 (ISO)
State Bank of India
Information Security Department,
State Bank Global IT Centre, Ground Floor, A Wing, Sector 11,
- (b) CBD Belapur, Navi Mumbai-400614 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 TRAINING: Service Provider shall train designated Bank officials on the configuration, operation/ functionalities, maintenance, support & administration for software, application architecture and components, installation, troubleshooting processes of the proposed Services as mentioned in this Agreement.
- 23.2 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.
- 23.3 SUCCESSORS AND ASSIGNS: This Agreement shall bind and inure to the benefit of the parties, and their respective successors and permitted assigns.
- 23.4 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.
- 23.5 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.
- 23.6 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.
- 23.7 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

- 23.8 PRIVACY: 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.
- 23.9 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.
- 23.10 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

By:
Name:
Designation:
Date:

_____ **Service Provider**

By:
Name:
Designation:
Date:

WITNESS:

1.

1.

2.

2.

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

ANNEXURE-A

DELIVERABLES/SCOPE OF WORK

Scope of Work and Payment Schedule

Comprehensive Security Review of Applications of Comprehensive Security Review (CSR) of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT-NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

Scope:

Details of Applications as per Appendix- E.

The Major Scope of the Security review of Applications as per Appendix-E is summarized below:

d) Secure Network Architecture Review

- d.1 Placement & Security of servers & network devices in SBI Network
- d.2 Firewall Rule Base Review
- d.3 Analysis of traffic monitoring (inward and outward traffic)

e) Application security review

- e.1 AppSec of application
- e.2 Role based Application review

f) VA/PT of all the Assets in scope

- f.1 VA – all the ports Internal, Credential Based

f.2 Both Internal and external PT

4 Configuration Audit

4.2. Configurations of All components such as OS, Database, Application server, web server etc. need to be reviewed (script based or manual) against Bank's Benchmark Document.

13 Process Review: Process flow including.

5.7. User management, privilege access etc., change control management, generation and checking of logs, incident management, flow of both to & fro traffic (its contents and the format in which it is travelling), storage at any point, password management, security environment, Compliance with RBI and local regulatory guidelines and Local Privacy Law and Bank's IT Policy and IS Policy and industry best practices.

5.8. Assessment of security risk involved in data being processed/handled at third party vendor's site/location covering end to end data flow to ensure CIA of information.

5.9. Review of each Database-on-database security perspective.

5.10. Review of Vendor/ Third Party Access management

5.11. In view of a few Applications under scope are with third party vendors, the selected ISSP must review the controls implemented by the vendor for Bank's Data processing as against Bank's set in controls at third party data processing of Bank's data.

5.12. Data Flow Diagram for all the Applications to be obtained and 'end to end' process review, specifically on third party locations, if any need to be carried out.

14 Source code review – Source code review wherever applicable as per the Appendix E

15 API Review: API review as per Appendix E.

16 Assessment of Forensic readiness and threat intelligence for individual Applications.

17 Compliance Review – as per Bank’s IT & IS Policy, Cyber Security Policy, RBI Guidelines and Best Global Security practices.

18 Confirmatory Review: If 100% compliance is not achieved in first round, the ISSP must do subsequent confirmatory reviews till the 100% closure of the observations. However, the 100% payment will be released after first round of confirmatory review on the condition of submitting an undertaking by the ISSP that, they will do the subsequent confirmatory review as a part of the assignment without any additional cost to the bank.

19 Preparedness for Ransomware:

- a) Assessment of Backup process
- b) Evaluation of enforcement of the defined back up process and Restoration testing.
- c) Compliance on patch management.

20 Data Security

- a) Assessment of Backup process
- b) Evaluation of enforcement of the defined back up process and Restoration testing.
- c) Compliance on patch management.

3. Deliverable for the Engagement:

- a) Hash Value and version number of every application (as advised by the Application Owner and for which it was reviewed) will be required to be incorporated in the final report for both initial and confirmatory review.
- b) Detailed Report highlighting vulnerabilities in the system. Technical vulnerability identified should provide: Risk impact (High, Medium, Low), possibility of occurrence (High/Medium/Low), ease of exploitation (Easy/Difficult/Very Difficult), specific mitigation measures keeping in view the criticality of the application, placement of the systems, type of the information passing over the channel, compensatory controls etc. If the service is vulnerable, screen shot/logs depicting vulnerability and change required in Secured Configuration Document may also be suggested.
- c) If any observation has been made which is as per the global best practices and not included in the Bank’s latest policies, RBI guidelines and IT Act, the relevant reference will have to be provided in the report by the ISSP.
- d) Both initial and final reports (after completion of the confirmatory review) will have to be presented application wise.
- e) A summary report (component wise) for all the applications/review areas (combined) will also be a part of both the reports.

- f) Both safe as well as unsafe findings are required to be listed along with the Mitigation tracker, listing the unsafe findings.
- g) An application and activity wise daily tracker to be provided to the Application Owner and Information Security Department.
- h) Recommendations for risk containment based on global best practices, Compliance to the latest SBI IT Policy, Information Security Policy, RBI guidelines, Local Regulatory Guidelines and IT Act 2008 etc. requirements would be required to be evaluated and reported.
- i) 100% confirmatory review will be required to be conducted. However, if the 100% confirmatory is not covered in first round, the Bank reserves the right to call the ISSP team to conduct other round(s) of confirmatory test, under prior intimation, if required, without any extra cost.
- j) Along with the soft copy of the final report, its printout with all pages signed by the authorized signatory under your company's seal must be submitted. The complete report should contain the following information also: -

Date of report

- o Exact period of conduct of the review and/or confirmatory review (as the case may be)
 - o Running page number for all pages
 - o Name and designation of the officials from Application Owner department with whom the findings had been discussed and finalized.
- k) If the ISSP resource is required to visit Bank's vendor partner's premises and/or for conducting White Box testing of the Source Code, the NDA will be signed between the ISSP resource and the Bank's vendor partner invariably.
 - l) E-Mail response from the Application Owner team may suffice in most of the cases of any reference in respect of the observations made. However, if required, the ISSP resource will be required to visit SBI for a one-on-one interaction on one or more instances with the Application Owner and/or Information Security Department.
 - m) ISSP to suggest risk containment / risk mitigation controls in case some of the remediation suggested in the report cannot be implemented because of technical or business-related reasons-application dependency.
 - n) **Delivery Schedule:** The initial review is to be completed and report to be submitted within 3 months from the date of Purchase Order. In case, after selection of L-1 ISSP, there is a delay in placing the formal Purchase Order, the Bank may provide a mail confirmation that the ISSP has been selected by the Bank for conducting the captioned review and the review process may be started on a notice of one day (formal Purchase Order may be placed by the Bank later).
 - o) All the payments shall be made by the Bank to the Selected Bidder except as otherwise provided in the bid after deducting all taxes including TDS, as per laid down provisions from time to time. All the payment shall be in Indian Rupees. The detailed payment terms are given below: -

| S.No. | Description | Terms of Payment |
|-------|--|------------------|
| 1 | After submission of Reports of 1 st Round of Review | 70% |
| 2 | After submission of Reports of Confirmatory Review | 30% |

**The initial review has to be completed within three months of the project inception.

DEPLOYMENT OF RESOURCES:

The bidders should deploy sufficient resources for review activities as per Skill-set and educational/professional criteria of this RFP within 10 days from the date of declaration of the successful bidder in the reverse auction . The detailed profile of the resources is to be uploaded in the e-tender portal .The defined resources may be interviewed to meet our desired requirements. If any resource is found unsuitable during the deployed period, the successful bidder has to provide an immediate replacement within 2 working days from the date of intimation. In case of resource resignation/termination during the deployed period, the successful bidder has to make necessary arrangement and provide an immediate alternative/replacement. In case the bidder fails to deploy as above, entire contract/assignment will be cancelled, and the penalty will be levied.

ANNEXURE-B

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. Transfer of Documentation

5.1 1 (One) months prior to expiry or within 2 (two) weeks of notice of termination of this Agreement Service Provider shall deliver to the Bank a full, accurate and up-to date set of Documentation that relates to any element of the Services as defined in Annexure A.

6. Transfer of Service Management Process

6.1 1 (One) 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.

7. Transfer of Knowledge Base

7.1 1(One) 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.

8. Transfer of Service Structure

8.1 1 (One) months prior to expiry or within 2 (two) weeks notice of termination of this Agreement Service Provider shall deliver to the Bank a full, accurate and up to date version of the following, as a minimum:

- (a) archive of records including:
 - (1) Questionnaire Packs;
 - (2) project plans and sign off;
 - (3) Acceptance Criteria; and
 - (4) Post Implementation Reviews.
- (b) programme plan of all work in progress currently accepted and those in progress;
- (c) latest version of documentation set;
- (d) Source Code (if appropriate) and all documentation to support the services build tool with any documentation for 'workarounds' that have taken place;
- (e) Source Code, application architecture documentation/diagram and other documentation;
- (f) Source Code, application architecture documentation/diagram and other documentation for Helpdesk; and
- (g) project plan and resource required to hand Service Structure capability over to the new team.

9. Transfer of Data

9.1 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.

9.2 Except where, pursuant to paragraph 14.1 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.

10. Training Services on Transfer

10.1 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.

10.2 The provision of any training services and/or deliverables and the charges for such services and/or deliverables shall be agreed between the parties.

10.3 Subject to paragraph 15.2 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.

10.4 Subject to paragraph 15.2 above, Service Provider shall schedule all necessary resources to fulfil the training plan, and deliver the training as agreed with the Bank.

10.5 SERVICE PROVIDER shall provide training courses on operation of licensed /open source software product at Bank's _____Premises, at such times, during business hours as Bank may reasonably request. Each training course will last for _____hours. Bank may enroll up to _____ of its staff or _____ employees of the new/replacement service provider in any training course, and Service Provider shall provide a hard copy of the Product (licensed or open sourced) standard training manual for each enrollee. Each training course will be

taught by a technical expert with no fewer than _____ years of experience in operating _____ software system. SERVICE PROVIDER shall provide the _____ training without any additional charges.

11. Transfer Support Activities

11.1 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.

11.2 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.

11.3 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.

11.4 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.

11.5 On the date of expiry Service Provider shall provide to the Bank refreshed versions of the materials required under paragraph 16.3 above which shall reflect the position as at the date of expiry.

11.6 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.

11.7 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.

12. Use of Bank Premises

12.1 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.

12.2 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).

ANNEXURE-C

Data Processing Agreement

≤ Applicable in case of activities for which selection of vendor/outsourcing of activities has been initiated involve access/sharing/transfer of Personal Data/PII of EU/UK NRI customers>

This Data Processing Agreement ("Agreement") forms part of the Contract for Services ("Principal Agreement") dated _____ between:

(i) State Bank of India ("Controller")

And

(ii) M/s. _____ ("Data Processor")

WHEREAS:

(A) State Bank of India (hereafter referred to as "SBI") acts as a Data Controller.

(B) SBI wishes to contract certain Services (provided in Schedule 1), which imply the processing of personal data (provided in Schedule 2), to the Data Processor.

The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) and any other data protection and privacy laws applicable to the Services.

(C) The Parties wish to lay down their rights and obligations (Processor obligations in Clause 3).

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation:

1.1 Unless otherwise defined herein, terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "Agreement" means this Data Processing Agreement and all schedules.

1.1.2 "Controller" has the meaning given to "data controller" in the UK Data Protection Act 1998 and "controller" in the General Data Protection Regulation (as applicable).

1.1.3 "Client" means a customer of State Bank of India.

1.1.4 "Data Protection Legislation" means as applicable, the UK Data Protection Act 1998, Directive 95/46/EC of the European Parliament and any laws or regulations implementing it, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and any equivalent or replacement law in the UK and any other data protection and privacy laws applicable to the Services.

1.1.5 "Data subject" has the meaning given to it in the Data Protection Legislation.

1.1.6 "Personal Data" has the meaning given to it in the Data Protection Legislation and relates only to Personal Data processed by a Contracted Processor on behalf of SBI pursuant to or in connection with the Principal Agreement in relation to the Services provided.

1.1.7 "Processor" means a data processor providing services to SBI.

1.1.8 "Subprocessor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of SBI in connection with the Agreement.

1.1.9 "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country.

1.1.10 "EEA" means the European Economic Area.

1.1.11 "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.

1.1.12 "GDPR" means EU General Data Protection Regulation 2016/679.

1.1.13 "Data Transfer" means:

1.1.13.1 a transfer of Personal Data from SBI to a Processor; or

1.1.13.2 an onward transfer of Personal Data from a Processor to a Subcontracted Processor, or between two establishments of a Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws).

1.1.14 "Services" means the services to be performed by the Processor described in the Principal Agreement (as provided in Schedule 1).

1.1.15 "Supervisory authority" has the meaning given to it in the Data Protection Legislation.

1.1.16 "Personal data breach" has the meaning given to it in the Data Protection Legislation.

1.1.17 "Personnel" means the personnel of the Processor, Subcontractors and Sub processors who provide the applicable Services; and

1.1.18 "Third country" has the meaning given to it in the Data Protection Legislation.

2. Processing of Personal Data:

2.1 In the course of providing Services to State Bank of India, the Processor may process Personal Data on behalf of State Bank of India.

2.2 Processor shall:

2.2.1 comply with all applicable Data Protection Laws in the Processing of Personal Data; and

2.2.2 not Process Personal Data other than on the relevant documented instructions of SBI.

3. PROCESSOR OBLIGATIONS:

3.1 Processor Personnel:

Processor shall take reasonable steps to ensure the reliability of any employee, agent or sub-processor who may have access to Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

3.1.1. The Processor shall process Personal Data only on the documented instructions from State Bank of India from time to time. State Bank of India shall notify the Processor of any amendments to existing instructions or additional instructions in relation to the processing of Personal Data in writing and Processor shall promptly comply with such instructions.

3.1.2. Notwithstanding clause 3.1, the Processor (and its Personnel) may process the Personal Data if it is required to do so by European Union law, Member State law or to satisfy any other legal obligations to which it is subject. In such circumstance, the Processor shall notify State Bank of India of that requirement before it processes the Personal Data, unless the applicable law prohibits it from doing so.

3.1.3. The Processor shall immediately notify State Bank of India if, in Processor's opinion, State Bank of India's documented data processing instructions breach the Data Protection Legislation. If and to the extent the Processor is unable to comply with any instruction received from State Bank of India, it shall promptly notify State Bank of India accordingly.

3.1.4. The purpose of the Processor processing Personal Data is the performance of the Services pursuant to the Principal Agreement.

3.2 Security:

3.2.1 Taking into account the nature, scope, context and purposes of Processing (provided in Schedule 2) as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to Personal Data implement appropriate technical and organizational measures (Processor obligations in Schedule 3) to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

3.2.2 In assessing the appropriate level of security, Processor shall take into account, in particular, risks related to processing of Personal Data.

3.2.3 The Processor shall use appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and protect against accidental loss or destruction of, or damage to, any Personal Data during processing activities. It shall implement and maintain the security safeguards and standards based on the IS policy of State Bank of India as updated and notified to the Processor by State Bank of India from time to time. The Processor will not decrease the overall level of security safeguards and standards during the term of this Agreement without State Bank of India's prior consent.

3.3 Sub-Processing:

3.3.1 The Processor shall not appoint (or disclose any Personal Data to) any Sub-Processors without prior written authorisation from State Bank of India. The Processor shall provide State Bank of India with [no less than [xx days] prior written (including email) notice before engaging a new Sub processor thereby giving State Bank of India an opportunity to object to such changes. If State Bank of India wishes to object to such new Sub processor, then State Bank of India may terminate the relevant Services without penalty by providing written notice of termination which includes an explanation of the reasons for such objection.

3.3.2 The Processor shall include in any contract with its Sub processors who will process Personal Data on State Bank of India's behalf, obligations on such Sub processors which are no less onerous than those obligations imposed upon the Processor in this Agreement relating to Personal Data. The Processor shall be liable for the acts and omissions of its Sub processors to the same extent to which the Processor would be liable if performing the services of each Sub processor directly under the terms of this Agreement.

3.4 Data Subject Rights:

Data subjects (SBI NRI customers) whose Personal Data is processed pursuant to this Agreement have the right to request access to and the correction, deletion or blocking of such Personal Data under Data Protection Legislation. Such requests shall be addressed to and be considered by State Bank of India responsible for ensuring such requests are handled in accordance with Data Protection Legislation.

3.4.1 Taking into account the nature of the Processing, Processor shall assist SBI by implementing appropriate technical and organisational measures (Processor obligations in Schedule 3), insofar as this is possible, for the fulfilment of SBI's obligations, as reasonably understood by SBI, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

3.4.2 In case Data Subject Requests are received by Processor, then the Processor shall:

3.4.2.1 promptly notify SBI if it receives a request from a Data Subject under any Data Protection Law in respect of Personal Data; and

3.4.2.2 ensure that it does not respond to that request except on the documented instructions of SBI or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws

3.4.2.3 inform SBI of that legal requirement before the Processor responds to the request.

3.5 Personal Data Breach:

3.5.1 Processor shall notify SBI without undue delay upon Processor becoming aware of a Personal Data Breach affecting Personal Data, providing SBI with sufficient information to allow SBI to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

3.5.2 Processor shall co-operate with SBI and take reasonable commercial steps as are directed by SBI to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

3.6 Data Protection Impact Assessment and Prior Consultation:

Processor shall provide reasonable assistance to SBI with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which SBI reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Personal Data by and taking into account the nature of the Processing and information available to, the Processors.

3.7 Deletion or return of Personal Data:

3.7.1 Subject to this section 3.7 Processor shall, promptly and in any event within <XX> business days of the date of cessation of any Services involving the Processing of Personal Data (the "Cessation Date"), delete all copies of those Personal Data.

3.7.2 Processor shall provide written certification to SBI that it has fully complied with this section 3.7 within < XX > business days of the Cessation Date.

3.8 Audit Rights:

The Processor shall make available to State Bank of India and any supervisory authority or their representatives the information necessary to demonstrate its compliance with this Agreement and allow for and contribute to audits and inspections by allowing State Bank of India, its Client, a supervisory authority or their representatives to conduct an audit or inspection of that part of the Processor's business which is relevant to the Services [on at least an annual basis (or more frequently when mandated by a relevant supervisory authority or to comply with the Data Protection Legislation) and] on reasonable notice, in relation to the Processing of Personal Data by the Processor.

3.9 Data Transfer:

The Processor may not transfer or authorize the transfer of Data to countries outside the EU/ India and/or the European Economic Area (EEA) without the prior written consent of SBI. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses / EU-US Privacy Shield for the transfer of personal data.

3.10 Records:

The Processor shall maintain written records of its data processing activities pursuant to providing the Services to State Bank of India in accordance with Data Protection Legislation.

3.11 Notify:

The Processor shall immediately and fully notify State Bank of India in writing of any communications the Processor (or any of its Sub processors) receives from third parties in connection with the processing of the Personal Data, including (without limitation) subject access requests or other requests, notices or other communications from individuals, or their representatives, or from the European Data Protection Board, the UK’s Information Commissioner’s Office (in the case of the United Kingdom) and/or any other supervisory authority or data protection authority or any other regulator (including a financial regulator) or court.

3.12 Agreement Termination:

Upon expiry or termination of this Agreement or the Services for any reason or State Bank of India’s earlier request, the Processor shall: (i) return to State Bank of India; and (ii) delete from all computer systems and other data storage systems, all Personal Data, provided that the Processor shall not be required to return or delete all or part of the Personal Data that it is legally permitted to retain. The Processor shall confirm to State Bank of India that it has complied with its obligation to delete Personal Data under this clause.

4. STATE BANK OF INDIA’S OBLIGATIONS:

State Bank of India shall:

4.1 in its use of the Services, process the Personal Data in accordance with the requirements of the Data Protection Legislation.

4.2 use its reasonable endeavours to promptly notify the Processor if it becomes aware of any breaches or of other irregularities with the requirements of the Data Protection Legislation in respect of the Personal Data processed by the Processor.

5. General Terms:

5.1 Confidentiality:

Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement (“Confidential Information”) confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

- (a) disclosure is required by law.
- (b) the relevant information is already in the public domain.

5.2 Notices:

All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

5.3 Governing Law and Jurisdiction:

5.3.1 This Agreement is governed by the laws of INDIA.

5.3.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of MUMBAI.

IN WITNESS WHEREOF, this Agreement is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out below.

For State Bank of India

Signature _____

Name _____

Title _____

Date Signed _____

For Processor M/s

Signature _____

Name _____

Title _____

Date Signed _____

SCHEDULE 1

1.1 Services

<<Insert a description of the Services provided by the Data Processor (under the Principal Service Agreement, where relevant)>>.

SCHEDULE 2

Personal Data

| Category of Personal Data | Category of Data Subject | Nature of Processing Carried Out | Purpose(s) of Processing | Duration of Processing |
|---------------------------|--------------------------|----------------------------------|--------------------------|------------------------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

SCHEDULE 3

Technical and Organisational Data Protection Measures

1. The Processor shall ensure that, in respect of all Personal Data it receives from or processes on behalf of SBI, it maintains security measures to a standard appropriate to:

1.1. the nature of the Personal Data; and

1.2. Safeguard from the harm that might result from unlawful or unauthorised processing or accidental loss, damage, or destruction of the Personal Data.

2. In particular, the Processor shall:

2.1. have in place, and comply with, a security policy which:

2.1.1. defines security needs based on a risk assessment.

2.1.2. allocates responsibility for implementing the policy to a specific individual (such as the Processor's Data Protection Officer) or personnel and is provided to SBI on or before the commencement of this Agreement.

2.1.3. ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice.

2.1.4. prevent unauthorised access to the Personal Data.

2.1.5. protect the Personal Data using pseudonymisation and encryption.

2.1.6. ensure the confidentiality, integrity and availability of the systems and services in regard to the processing of Personal Data.

2.1.7. ensure the fast availability of and access to Personal Data in the event of a physical or technical incident.

2.1.8. have in place a procedure for periodically reviewing and evaluating the effectiveness of the technical and organisational measures taken to ensure the safety of the processing of Personal Data.

2.1.9. ensure that its storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded (including paper records and records

stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled.

2.1.10. have secure methods in place for the transfer of Personal Data whether in physical form (for example, by using couriers rather than post) or electronic form (for example, by using encryption).

2.1.11. password protect all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure, and that passwords are not shared under any circumstances.

2.1.12. not allow the storage of the Personal Data on any mobile devices such as laptops or tablets unless such devices are kept on its premises at all times.

2.1.13. take reasonable steps to ensure the reliability of personnel who have access to the Personal Data.

2.1.14. have in place methods for detecting and dealing with breaches of security (including loss, damage, or destruction of Personal Data) including:

2.1.14.1. having a proper procedure in place for investigating and remedying breaches of the GDPR; and

2.1.14.2. notifying SBI as soon as any such security breach occurs.

2.1.15. have a secure procedure for backing up all Personal Data and storing back-ups separately from originals; and

2.1.16. adopt such organisational, operational, and technological processes and procedures as are required to comply with the requirements of ISO/IEC 27001:2013 and SBI’s Information Security Policy as appropriate.

At the time of signing this Agreement, the Processor has the following technical and organizational measures in place: (To be vetted by SBI)

| S. No | Controls to be implemented | Compliance (Yes / No) | If under implementation, give date by which implementation will be done |
|-------|---|-----------------------------------|---|
| 1 | Whether the Processor has Information security policy in place with periodic reviews? | | |
| 2 | Whether the Processor have | a. Business Continuity Management | |
| | | b. Backup management | |

| S. No | Controls to be implemented | Compliance (Yes / No) | If under implementation, give date by which implementation will be done |
|-------|---|--|---|
| | operational processes with periodic review, including but not limited to: | c. Desktop/system/server/network device hardening with baseline controls | |
| | | d. Patch Management | |
| | | e. Port Management Media Movement | |
| | | f. Log Management | |
| | | g. Personnel Security | |
| | | h. Physical Security | |
| | | i. Internal security assessment processes | |
| 3 | Whether a proper documented Change Management process has been instituted by the Processor? | | |
| 4 | Whether the Processor has a documented policy and process of Incident management /response? | | |
| 5 | Whether the Processor's environment is suitably protected from external threats by way of: | a. Firewall | |
| | | b. WAF | |
| | | c. IDS/IPS | |
| | | d. AD | |
| | | e. AV | |
| | | f. NAC | |
| | | g. DLP | |
| | | h. Any other technology | |
| 6 | Whether rules are implemented on Firewalls of the Processor environment as per an approved process? | | |
| 7 | Whether firewall rule position is regularly monitored for presence of any vulnerable open port or any-any rule? | | |
| 8 | Whether proper log generation, storage, management and analysis happens for the Processor application? | | |

| S. No | Controls to be implemented | Compliance (Yes / No) | If under implementation, give date by which implementation will be done |
|-------|--|------------------------------|---|
| 9 | Is the Processor maintaining all logs for forensic readiness related to: | a. Web | |
| | | b. Application | |
| | | c. DB | |
| | | d. Configuration | |
| | | e. User access | |
| 10 | Whether the Processor maintains logs for privileged access to their critical systems? | | |
| 11 | Whether privilege access to the Processor environment is permitted from internet? | | |
| 12 | Whether the Processor has captive SOC or Managed Service SOC for monitoring their systems and operations? | | |
| 13 | Whether the Processor 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? | | |
| 14 | Whether Processor has deployed secure environments for their applications for: | a. Production | |
| | | b. Disaster recovery | |
| | | c. Testing environments | |
| 15 | Whether the Processor follows the best practices of creation of separate network zones (VLAN Segments) for: | a. Web | |
| | | b. App | |
| | | c. DB | |
| | | d. Critical applications | |
| | | e. Non-Critical applications | |
| | | f. UAT | |
| 16 | Whether the Processor configures access to officials based on a documented and approved Role Conflict Matrix? | | |
| 17 | Whether Internet access is permitted on: | a. Internal servers | |
| | | b. Database servers | |
| | | c. Any other servers | |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

| S. No | Controls to be implemented | Compliance (Yes / No) | If under implementation, give date by which implementation will be done |
|--------------|--|------------------------------|--|
| 18 | Whether the Processor has deployed a dedicated information security team independent of IT, reporting directly to MD/CIO for conducting security related functions & operations? | | |
| 19 | Whether CERT-IN Empaneled ISSPs are engaged by the third party for ensuring security posture of their application? | | |
| 20 | Whether quarterly vulnerability assessment and penetration testing is being done by the Processor for their infrastructure? | | |
| 21 | Whether suitable Security Certifications (ISO, PCI-DSS etc.) of the security posture at vendor environment are in place? | | |
| 22 | Whether the Processor has deployed any open source or free software in their environment? | | |
| | If yes, whether security review has been done for such software? | | |
| 23 | Whether the data shared with the Processor is owned by SBI (SBI = Information Owner)? | | |
| 24 | Whether the data shared with the Processor is of sensitive nature? | | |
| 25 | Whether the requirement and the data fields to be stored by the Processor is approved by Information Owner? | | |
| 26 | Where shared, whether the bare minimum data only is being shared? (Please document the NEED for sharing every data field) | | |
| 27 | Whether the data to be shared with Processor will be encrypted as per industry best standards with robust key management? | | |
| 28 | Whether the Processor is required to store the data owned by State Bank? | | |
| 29 | Whether any data which is permitted to be stored by the Processor will be completely erased after processing by the Processor at their end? | | |
| 30 | Whether the data shared with the Processor is stored with encryption (Data at rest encryption)? | | |

| S. No | Controls to be implemented | Compliance (Yes / No) | If under implementation, give date by which implementation will be done |
|-------|--|--|---|
| 31 | Whether the data storage technology (Servers /Public Cloud/ Tapes etc.) has been appropriately reviewed by IT AO? | | |
| 32 | Whether the Processor is required to share SBI specific data to any other party for any purpose? | | |
| 33 | Whether a system of obtaining approval by the Processor from the IT Application Owner is put in place before carrying out any changes? | | |
| 34 | Whether Processor is permitted to take any crucial decisions on behalf of SBI without written approval from IT Application Owner? | | |
| | If not, are such instances being monitored? IT Application Owner to describe the system of monitoring such instances. | | |
| 35 | Whether Application Owner has verified that the Processor has implemented efficient and sufficient preventive controls to protect SBI's interests against any damage under section 43 of IT Act? | | |
| 36 | Whether the selection criteria for awarding the work to Processor vendor is based on the quality of service? | | |
| 37 | Whether the SLA/agreement between SBI and the Processor contains these clauses: | a. Right to Audit to SBI with scope defined | |
| | | b. Adherence by the vendor to SBI Information Security requirements including regular reviews, change management, port management, patch management, backup management, access management, log management etc. | |
| | | c. Right to recall data by SBI. | |
| | | d. Regulatory and Statutory compliance at vendor site. | |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

| S. No | Controls to be implemented | | Compliance (Yes / No) | If under implementation, give date by which implementation will be done |
|-------|----------------------------|---|-----------------------|---|
| | | Special emphasis on section 43A of IT Act 2000 apart from others. | | |
| | | e. Availability of Compensation clause in case of any data breach or incident resulting into any type of loss to SBI, due to vendor negligence. | | |
| | | f. No Sharing of data with any third party without explicit written permission from competent Information Owner of the Bank including the Law Enforcement Agencies. | | |

XXXXX

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.

2. 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 | | |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

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 whomsoever 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

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department

Detailed Scope of the applications: **Comprehensive Security Review (CSR) of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO, IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department**

CSR 2024-25– Scope collection document

Name of the Department: Software Factory, Software Factory (Infra & Operations)

| S/ N | Name of Application along with APM ID | Sub module Name | Criticality of Application | Type of application (web/ mobile /backend process etc | Exposed to (Internet/ Public NW) – Yes/ No | No. of Devices for VA and SCD | | | | | Source Code | | AppSec | | No. of web Services | No. of Firewall rules. (We are in touch with NSPM team to get the details and will share the same) | No. of APIs hosted |
|---------|--|-----------------|----------------------------|---|--|-------------------------------|----|-----|-----|-------|-------------|------------------------------------|------------------|----------------------------|---------------------|--|--------------------|
| | | | | | | OS | DB | App | Web | Total | LoC | Language | No of user roles | Input pages/ Dynamic pages | | | |
| 1 | An IT Application for OTS application (APP05610) | OTSS | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 7500 | ASP.Net C# | 7 | 8 | 0 | | 0 |
| 2 | ATR Tracking Portal (RCaS_Info_1512) | ATP | Low | WEB | NO | 4 | 2 | 2 | 0 | 4 | 26792 | Java Oracle ADF | 6 | 10 | 0 | | 0 |
| 3 | BCDM Workflow (Webs_Tran_1506) | BCDM | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 25000 | Java Oracle ADF | 6 | 15+ | 1 | | 0 |
| 4 | Branch Darpan (Webs_Info_1399) | Branch Darpan | Low | WEB | NO | 4 | 2 | 2 | 0 | 4 | 5000 | PHP | 4 | 10 | 0 | | 0 |
| 5 | Branch eRegister (Serv_Info_447) | eRegister | Low | WEB | NO | 4 | 2 | 2 | 0 | 4 | 60000 | ASP.Net C# | 2 | 30+ | 0 | | 0 |
| 6 | Branch Manager Monthly Certificate (Serv_Tran_567) | BMMC | Low | WEB | NO | 4 | 2 | 2 | 0 | 4 | 30000 | MVC .Net C# | 4 | 30+ | 0 | | 0 |
| 7 | Compliance department (Serv_Info_438) | Comport | Low | WEB | NO | 4 | 2 | 2 | 0 | 4 | 29424 | Java, Springboot, react js, Oracle | 28 | 25 | 0 | | 0 |
| 8 | Controllers Visit System (Serv_Info_458) | CVS | Low | WEB | NO | 4 | 2 | 2 | 0 | 4 | 30000 | .Net VB | 3 | 30+ | 0 | | 4 |
| 9 | Corporate Tie Ups Portal (Webs_Info_2171) | CTUP | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 5000 | .Net | 2 | 2 | 0 | | 0 |
| 10 | Counterfeit Currency Reporting (Serv_Tran_551) | CCR | Low | WEB | NO | 4 | 2 | 2 | 0 | 4 | 50000 | .Net C# | 6 | 4 | 0 | | 0 |
| 11 | CRMD Portal for regulatory return (APP04013) | NA | Medium | WEB | NO | 6 | 2 | 2 | 2 | 6 | 32000 | .Net | 4 | 10 | 1 | | 0 |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | | | | | | | | | | | | |
|----|---|---------------------------------|--------|-----|-----|----|---|----|---|----|--------|----------------------------|----|-----|----|--|----|
| 12 | CRPD Lateral Recruitment Portal (Webs_Tran_1832) | CRPD Lateral Recruitment Portal | Medium | WEB | YES | 16 | 2 | 8 | 6 | 16 | 100000 | PHP | 4 | 30+ | 0 | | 0 |
| 13 | CS Email Segregation (Serv_Info_2650) | CS Email Segregation | Low | WEB | NO | 8 | 4 | 2 | 2 | 8 | 8000 | .Net | 1 | 1 | 0 | | 0 |
| 14 | Dashboard for calculation and recovery of charges (APP04305) | NA | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 26783 | .Net | 3 | 22 | 1 | | 0 |
| 15 | Document Library System (APP04520) | NA | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 20300 | Angular and php | 6 | 12 | 30 | | 25 |
| 16 | EasyApproval 3.0 (APP04326) | NA | Medium | WEB | NO | 28 | 2 | 22 | 4 | 28 | 180000 | Java, Spring boot, Angular | 2 | 7 | 0 | | 0 |
| 17 | ENTERPRISE DAK MANAGEMENT SYSTEM (Webs_Tran_2141) | E DAK | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 100000 | .Net | 10 | 2 | 0 | | 0 |
| 18 | Exception Report Monitoring System (Webs_Info_2060) | ERMS | Low | WEB | NO | 8 | 2 | 4 | 2 | 10 | 10000 | .NET | 6 | 4 | 0 | | 0 |
| 19 | FCC Portal (L&A_Info_2524) | FCC Portal | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 5000 | Java Angular | 3 | 4 | 0 | | 0 |
| 20 | Financial Soundness Indicator (A&R_Info_2550) | FSI | Medium | WEB | YES | 6 | 2 | 2 | 2 | 6 | 92718 | Python | 50 | 15 | 0 | | 0 |
| 21 | Framework for Revival and Rehabilitation of MSMEs (A&R_Info_2567) | MSME Portal | Medium | WEB | NO | 6 | 2 | 2 | 2 | 6 | 10000 | ASP.Net C# | 6 | 15 | 1 | | 0 |
| 22 | Fraud Database Monitoring System (Serv_Info_2727) | FDMS | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 30000 | .Net C# MVC | 2 | 10 | 0 | | 0 |
| 23 | FRT RBI Return (APP03924) | FSI | Low | WEB | YES | 6 | 2 | 2 | 2 | 6 | 92718 | Python | 50 | 15 | 0 | | 0 |
| 24 | GITC GRC (RCaS_Info_1965) | GITC GRC | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 10000 | .NET | 2 | 5 | 0 | | 0 |
| 25 | GMS Portal (A&R_Info_2566) | GMS | Medium | WEB | NO | 6 | 2 | 2 | 2 | 6 | 50000 | .Net C# | 5 | 15 | 1 | | 0 |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | | | | | | | | | | | | |
|----|---|-----------------------|--------|-----|----|---|---|---|---|---|--------|-------------------|----|-----|---|--|---|
| 26 | HR website. (Webs_Info_2628) | HRWeb | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 5000 | .Net C# | 2 | 6 | 0 | | 0 |
| 27 | Insurance Claim Reporting System (Serv_Info_449) | ICRS | Low | WEB | NO | 2 | 1 | 1 | 0 | 2 | 5000 | .Net VB | 1 | 6 | 0 | | 0 |
| 28 | IS Concurrent Audit Application (RCaS_Info_410) | ISCA | Low | WEB | NO | 4 | 2 | 2 | 0 | 4 | 5000 | .Net C# | 4 | 4 | 0 | | 0 |
| 29 | iTRAMS - Intranet based Training Management System (T/L_Info_613) | No | Low | WEB | NO | 4 | 2 | 2 | 0 | 4 | 461121 | ASP.NET Web Forms | 10 | 145 | 0 | | 0 |
| 30 | KCC-ISS Bank's Portal (APP05945) | KCC ISS Bank's Portal | Medium | WEB | NO | 6 | 2 | 2 | 2 | 6 | 0 | C#, JavaScript | 4 | 16 | 0 | | 0 |
| 31 | LITIGATION MANAGEMENT SYSTEM (Webs_Info_1616) | LITMAS | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 60000 | Java, Angular | 11 | 50 | 0 | | 0 |
| 32 | Locker Allocation Management Project (APP04120) | LAMP | Medium | WEB | NO | 8 | 4 | 2 | 2 | 8 | 70000 | .Net C# | 5 | 100 | 3 | | 3 |
| 33 | MPFI DSB THROUGH BRANCH CHANNEL (A&R_Info_2730) | NA | Medium | WEB | NO | 6 | 2 | 2 | 2 | 6 | 8899 | .Net | 3 | 15 | 1 | | 0 |
| 34 | Online Branch Security Audit (RCaS_Tran_1508) | OBSA | Low | WEB | NO | 4 | 2 | 2 | 0 | 4 | 80000 | .Net VB | 6 | 6 | 0 | | 0 |
| 35 | PORTAL FOR TRACKING THE STATUS OF NHRC CASES (Webs_Info_2181) | PTSNC | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 3000 | .Net | 2 | 2 | 0 | | 0 |
| 36 | POTOMAS POs TOs Monitoring and Advisory System (T/L_Info_614) | POTOMAS | Low | WEB | NO | 2 | 1 | 0 | 1 | 2 | 33967 | ASP.NET MVC | 5 | 95 | 0 | | 0 |
| 37 | Pragati Portal (APP05582) | PRAGATI PORTAL | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 20000 | .NET | 5 | 19 | 1 | | 0 |
| 38 | PSL Fund Tracking Portal (Serv_Info_2364) | PSLFT | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 20000 | Java React | 7 | 10 | 0 | | 0 |
| 39 | RAJBHASHA WEBSITE (Webs_Info_1825) | RAJBHASH A | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 5000 | .NET | 1 | 1 | 0 | | 0 |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | | | | | | | | | | | | |
|----|--|------------|--------|-----------------|----|----|---|----|---|----|--------|------------------|----|-----|---|--|---|
| 40 | REH Gyan (Webs_Info_2242) | REH Gyan | Low | WEB | NO | 4 | 2 | 2 | 0 | 4 | 5000 | Java | 3 | 7 | 0 | | 0 |
| 41 | Retired Employees Medical Benefit Scheme Revised (Serv_Info_446) | REMBS | Low | WEB | NO | 4 | 2 | 2 | 0 | 4 | 30000 | ASP.Net C# | 6 | 20+ | 0 | | 0 |
| 42 | SBI Intelligent Voice Assistant (Inno_Info_1626) | SIVA | Low | BACKEND PROCESS | NO | 24 | 8 | 16 | 0 | 24 | 5000 | Java | 0 | 0 | 0 | | 0 |
| 43 | SBI QUIZ Application (T/L_Info_601) | QUIZ | Low | WEB | NO | 4 | 2 | 2 | 0 | 4 | 3500 | Java (JEE) | 2 | 10 | 0 | | 0 |
| 44 | SME Gyan (Know_Info_1563) | SME Gyan | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 15000 | Java | 3 | 20+ | 0 | | 0 |
| 45 | Staff Productivity Metric (Webs_Info_2646) | SPM | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 15000 | Java | 4 | 10 | 0 | | 0 |
| 46 | Training Dashboard_SBIICM (T/L_Info_605) | SBTRACS | Low | WEB | NO | 4 | 2 | 2 | 0 | 4 | 2412 | ASP.NET MVC | 5 | 35 | 0 | | 4 |
| 47 | UAT Tracking Tool (Webs_Info_1852) | UAT PORTAL | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 10000 | .NET | 6 | 7 | 0 | | 2 |
| 48 | Vigilance Case tracking System (Serv_Info_437) | VCTS | Medium | WEB | NO | 6 | 2 | 2 | 2 | 6 | 25000 | Java Oracle ADF | 13 | 15+ | 1 | | 0 |
| 49 | VPN WORKFLOW (Webs_Infr_2707) | NA | Low | WEB | NO | 6 | 2 | 2 | 2 | 6 | 32532 | .Net | 6 | 38 | 0 | | 0 |
| 50 | WEB PORTAL FOR REGULATORY RETURNS (A&R_Info_2568) | WPRR | Medium | WEB | NO | 6 | 2 | 2 | 2 | 6 | 10000 | .Net C# | 5 | 0 | 0 | | 0 |
| 51 | GITC HR DASHBOARD (T/L_Info_602) | GITCHR | Low | WEB | NO | 4 | 2 | 2 | 0 | 4 | 150000 | Java, Spring MVC | 4 | 240 | 0 | | 0 |

Count of External Facing IPs: 6 (3 DC + 3 DR)

Details of Third Party / Vendors where Sensitive data flows outside Bank

| Name of the Third Party/ Vendor | Location Address | Services offered / Purpose of Integration | Supply Chain Control Point Report Available / To be Reviewed |
|---------------------------------|------------------|---|--|
| NA | NA | NA | NA |



CSR SCOPE-2024-25

Department Name: Internet Banking

1. Application Details

| Sr. No | Name of Application | Criticality rating of application | Type of application (web/mobile /backend process | Exposed to (Internet/ Public NW) | Source Code | | App sec | | No. of web Services/API | Firewall Rules | Vendor Name | Vendor Location |
|--------|---------------------|-----------------------------------|--|----------------------------------|--------------------|------------|------------------|----------------------------|-------------------------|-------------------------------------|-------------|-----------------|
| | | | | | LoC (Line of code) | Language | No of user roles | Input pages/ Dynamic pages | | | | |
| 1 | Retail | H | Web | Internet | 982545 | Java | 01 | 2996 | 17 | Permanent-1769 Temp-1520 | TechM | GITC/Chennai |
| 2 | Merchant | H | Web | Internet | 70779 | Java | 02 | 10 | 16 | | TechM | GITC/Chennai |
| 3 | Prelogin | H | Web | Internet | 76754 | Java | NA | 25 | 2 | | TechM | GITC/Chennai |
| 4 | CCS | H | Platform | Intranet | 25308 | IIB | NA | NA | 13 | | TechM | GITC/Chennai |
| 5 | YONO Lite | H | Mobile App | Internet | 800000 | Java, Kony | 01 | 400 | 480 | FARs for mobility- Permanent-127 | TechM, UST | GITC/Chennai |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|-----------|--|--|
| | | | | | | | | | | Temp- 720 | | |
| | | | | | | | | | | NA | | |

| Name of Application | No. of Devices for VA/SCD | | | | | |
|------------------------|--|--------------------|--------------------|--------------------|---------------------------|----------------------|
| | OS | DB | App | Web | Others | Total no. of servers |
| | (DC+DR separately) | (DC+DR separately) | (DC+DR separately) | (DC+DR separately) | (DC+DR separately) | (DC+DR separately) |
| Retail | AIX 7.3, Solaris 11.4 | 3+3 | 16+16 | 12+12 | 13+13 | 44+44 |
| Merchant | AIX 7.3, Solaris 11.4 | 3+3 | 15+15 | 10+10 | 5+5 | 33+33 |
| Prelogin/onlinesbi.sbi | AIX 7.3, Solaris 11.4 | 0+0 | 4+4 | 4+4 | 0+0 | 8+8 |
| CCS | AIX 7.3, Solaris 11.4 | 3+3 | 12+12 | 0+0 | 0+0 | 15+15 |
| YONO Lite | AIX-16, RHEL-19 (DC) AIX-16, RHEL-19 (DR) Solaris- 3+3+3 (DC+DR+NDR) | 3+3+3 (DC+DR+NDR) | 19+19 (DC+DR) | 16+16 (DC+DR) | 8+8 Load Balancer (DC+DR) | 84+84+6 |



Number of public facing applications: 5
 Number of intranet applications: 0

2. Number of 3rd party products (e.g. RadWare, Kony etc):

| Name of 3 rd party product | Name of the vendor | Number of servers in setup | Used for/Purpose |
|---------------------------------------|--------------------|----------------------------|----------------------------------|
| Load Balancer – Alteon 8420 XL | Radware | DC-18, DR -18 | For load balancing WEB Traffic |
| IBM Power 8 | IBM | 39 (DC-21 and DR-18) | IBM Rack for APP and WEB Servers |
| IBM Power 9 | IBM | 17 (DC-5 and DR-12) | IBM Rack for APP and WEB Servers |
| KONY Middleware version: 8.4 | Temenos | 19 (Kony : Web+App) | MiddleWare |

3. Number of Merchant Aggregators/Sub-merchants/Direct merchants

| Name of the application | Number of merchants integrated | Remarks |
|-------------------------|--------------------------------|---------|
| | | |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | |
|-----------|-----|--------------------------|
| Merchant | 681 | Direct Merchants(active) |
| YONO Lite | 2 | Merchant Aggregators |

Number of new applications added since last CSR (specify name of application as well): NIL

List of URLs of all the application:

| Application Name | Environment (PROD/UAT) | URL |
|------------------|------------------------|---|
| Retail | UAT | https://retail.onlinesbi.sbi |
| Retail | PROD | https://retail.onlinesbi.sbi |
| Merchant | UAT | https://uatmerchant.onlinesbi.sbi |
| Merchant | PROD | https://merchant.onlinesbi.sbi |
| Prelogin | UAT | https://www.onlinesbi.sbi |
| Prelogin | PROD | https://www.onlinesbi.sbi |
| CCS | UAT | https://soa.onlinesbi.sbi |
| CCS | PROD | https://soa.onlinesbi.sbi |
| YonoLite | PROD | https://mobilityretail.sbi/, https://api.yonolite.sbi |
| YonoLite | UAT | https://api.uatyonolite.sbi |

We confirm that, all the Existing Applications owned/managed by our department are included in the list and that all the details provided above are correct.



CSR 2025– Scope Collection Document

Department Name: CMP & SCFU

| Sr No | Name of Application | Criticality rating of application | Criticality score of application out of 42 | Submodule Name | Type of application (web/mobile/backend process) | Exposed to (Internet/Public NW) | No. of Devices for VA/SCD | | | | | Source Code | | App sec | | No. of web Services | No. Of Firewall Rules | No. of API | Vendor Name | Vendor Location | Details of vendor support |
|-------|---------------------|-----------------------------------|--|----------------|--|---------------------------------|---------------------------|--------------|--------------|--------------|-------|--------------------|----------|------------------|---------------------------|---------------------|-----------------------|------------|---------------|-----------------|---------------------------|
| | | | | | | | OS | DB | App | Web | Total | LoC (Line of code) | Language | No of user roles | Input pages/Dynamic pages | | | | | | |
| 1 | FastPlus | High | 40 | Payment | Web | Yes | 16 | DC-2 DR-2 | DC-3 DR-3 | DC-3 DR-3 | 16 | 55L | JAVA | 11 | Input Page | 1 | 847 | 19 | Tech Mahindra | GITC | Infra/Dev and Support |
| | | | 33 | Collectio n | Web | Yes | | | | | | 5L | | 5 | | 0 | | 10 | | | |
| | | | 33 | Mandate | Web | Yes | | | | | | 6L | | 2 | | 2 | | 5 | | | |

Number of public facing applications: 4

Number of intranet applications: 2

Number of 3rd party products (e.g Radware , Dynatrace etc.) : 9

| Sr No | Name of 3 rd party product | Name of the vendor | Number of servers in setup | Used for/Purpose |
|-------|---------------------------------------|--------------------|----------------------------|----------------------------|
| 1 | IBM WAS/IHS 8.5 | IBM | 22 (SCFU 12+ CMP 10) | Web/Middleware application |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | |
|---|--------------------------------------|-------------|---|--|
| 2 | Oracle 19C Rac Database | Oracle | 20 (SCFU 12 + CMP 8) | SBI FastPlus and SCF Database |
| 3 | Radware Load Balancer | Radware | 08 (SCFU 04 + CMP 04) | Web traffic Load Balancing (Fast Plus) |
| 4 | Oracle 19C | Oracle | 04 (CMP) | Database |
| 5 | Dynatrace | Dynatrace | 0 | Monitoring |
| 6 | Weblogic / OHS | Oracle | 06 (RelID H2H) | Web/Middleware application |
| 7 | MongoDB | Open Source | 02 (RelID H2H) | RelID Database |
| 8 | Nginx | Open Source | 02 (RelID H2H) | 2 for RelID Web Server and 12 containers of SCF Revamp |
| 9 | Spring Boot (Apache Tomcat Embadded) | VMWare | 150 (containers running on Kubernetes Host) | SCFU Revamp Application Server |

File sharing process SOP: H2H, SFTP/ SFG SFTP

Key sharing process SOP: Email / Portal

Number of merchants: None

Number of new applications added since last CSR (specify name of application as well): None



List of URLs of all the application:

| Environment | Environment present/absent (Applicable/ Not Applicable) | Application Name | URL |
|----------------------|---|------------------|--|
| SBI Fast Plus | | | |
| UAT | Present | SBI FastPlus | https://m.fastplusuat.onlinesbi.com:8443/bulkpaymentapi/cmp/services/ https://m.fastplusuat.onlinesbi.com:8443/RealTimeEnquiryServices/Service/Enquiry/ https://m.fastplusuat.onlinesbi.com:8443/RealTimePaymentServices/Service/Payment/ https://m.fastplusuat.onlinesbi.com:8443/SAPPaymentServices/services/SBISoapSrc?wsdl https://m.fastplusuat.onlinesbi.com:8443/SBIfastplusAPI/mpat/userValidation https://m.fastplusuat.onlinesbi.com:8443/SBIfastplusAPI/mpat/updateTransaction |



| Environment | Environment present/absent (Applicable/ Not Applicable) | Application Name | URL |
|-------------|---|------------------|--|
| | | | <p>https://m.fastplusuat.onlinesbi.com:8443/SBITokenServices/token/getToken/</p> <p>https://m.fastplusuat.onlinesbi.com/ybPayments/getReqRefencrypt</p> <p>https://m.fastplusuat.onlinesbi.com/ybpending/payloadPendingApprovalTxn</p> <p>https://m.fastplusuat.onlinesbi.com/ybPayments/getReqRefdecrypt</p> <p>https://m.fastplusuat.onlinesbi.com/ybPayments/getReqRefencrypt</p> <p>https://m.fastplusuat.onlinesbi.com/ybpayables/payloadUpcomingPay</p> <p>https://m.fastplusuat.onlinesbi.com/ybPayments/getReqRefdecrypt</p> |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| Environment | Environment present/absent (Applicable/ Not Applicable) | Application Name | URL |
|-------------|---|------------------|---|
| | | | <p>https://m.fastplusuat.onlinesbi.com/ybPayments/getReqRefencrypt</p> <p>https://m.fastplusuat.onlinesbi.com/ybuseraccess/fechUserAccesslevel</p> <p>https://m.fastplusuat.onlinesbi.com/ybPayments/getReqRefdecrypt</p> <p>https://m.fastplusuat.onlinesbi.com/ybPayments/getReqRefencrypt</p> <p>https://m.fastplusuat.onlinesbi.com/digitalsso/requestRefGenerateReq</p> <p>https://m.fastplusuat.onlinesbi.com/ybPayments/getReqRefdecrypt</p> <p>https://newcmp.onlinesbi.com:8444/SBIGovTokenService/token/getToken</p> <p>https://newcmp.onlinesbi.com:8444/SBIGovIntroService/introService/sendPayLoad</p> |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| Environment | Environment present/absent (Applicable/ Not Applicable) | Application Name | URL |
|-------------|---|------------------|---|
| | | | https://newcmp.sbi:8443/SbiGovIREPSService/ireps/sendData https://newcmp.sbi:8443/SbiGovIREPSService/ireps/sendMerchantInq https://newcmp.sbi:8443/SbiGovIREPSService/ireps/sendBalanceInq https://newcmp.sbi:8443/ITRO_SBICRM/itrocrm/userdetails https://newcmp.sbi:8444/SBIITDService/ITDService/validatePan https://newcmp.sbi:8444/SBIITDService/ITDService/sendPanAccData https://newcmp.sbi:8443/ITRO_SBICRM/itrocrm/getToken |
| PRE-PROD | Present | SBI FastPlus | https://newcmp.sbi:8443/bulkpaymentapi/cmp/services/ https://newcmp.sbi:8443/RealTimeEnquiryServices/Service/Enquiry/ |



| Environment | Environment present/absent (Applicable/ Not Applicable) | Application Name | URL |
|-------------|---|------------------|--|
| | | | <p>https://newcmp.sbi:8443/RealTimePaymentServices/Service/Payment/</p> <p>https://newcmp.sbi:8443/SAPPaymentServices/services/SBISoapSrvc?wsdl</p> <p>https://newcmp.sbi:8443/SBIfastplusAPI/mpat/userValidation</p> <p>https://newcmp.sbi:8443/SBIfastplusAPI/mpat/updateTransaction</p> <p>https://newcmp.sbi:8443/SBITokenServices/token/getToken/</p> <p>https://newcmp.sbi/ybPayments/getReqRefencrypt</p> <p>https://newcmp.sbi/ybpending/payloadPendingApprovalTxn</p> |



| Environment | Environment present/absent (Applicable/ Not Applicable) | Application Name | URL |
|-------------|---|------------------|---|
| | | | <p>https://newcmp.sbi/ybPayments/getReqRefdecrypt</p> <p>https://newcmp.sbi/ybPayments/getReqRefencrypt</p> <p>https://newcmp.sbi/ybpayables/payloadUpcoming Pay</p> <p>https://newcmp.sbi/ybPayments/getReqRefdecrypt</p> <p>https://newcmp.sbi/ybPayments/getReqRefencrypt</p> <p>https://newcmp.sbi/ybuseraccess/fetchUserAccesslevel</p> <p>https://newcmp.sbi/ybPayments/getReqRefdecrypt</p> |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| Environment | Environment present/absent (Applicable/ Not Applicable) | Application Name | URL |
|-------------|---|------------------|---|
| | | | https://newcmp.sbi/ybPayments/getReqRefencrypt https://newcmp.sbi/digitalssso/requestRefGenerateReq https://newcmp.sbi/ybPayments/getReqRefdecrypt https://newcmp.onlinesbi.com:8444/SBIGovTokenService/token/getToken https://newcmp.onlinesbi.com:8444/SBIGovIntroService/introService/sendPayLoad https://newcmp.sbi:8443/ITRO_SBICRM/itrocrm/userdetails https://newcmp.sbi:8443/ITRO_SBICRM/itrocrm/getToken |
| SIT | Present | SBI FastPlus | https://newcmp.sbi:8443/bulkpaymentapi/cmp/services/ https://newcmp.sbi:8443/RealTimeEnquiryServices/Service/Enquiry/ |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| Environment | Environment present/absent (Applicable/ Not Applicable) | Application Name | URL |
|-------------|---|------------------|--|
| | | | <p>https://newcmp.sbi:8443/RealTimePaymentServices/Service/Payment/</p> <p>https://newcmp.sbi:8443/SAPPaymentServices/services/SBISoapSrvc?wsdl</p> <p>https://newcmp.sbi:8443/SBIfastplusAPI/mpat/userValidation</p> <p>https://newcmp.sbi:8443/SBIfastplusAPI/mpat/updateTransaction</p> <p>https://newcmp.sbi:8443/SBITokenServices/token/getToken/</p> <p>https://newcmp.sbi/ybPayments/getReqRefencrypt</p> <p>https://newcmp.sbi/ybpending/payloadPendingApprovalTxn</p> |



| Environment | Environment present/absent (Applicable/ Not Applicable) | Application Name | URL |
|-------------|---|------------------|---|
| | | | <p>https://newcmp.sbi/ybPayments/getReqRefdecrypt</p> <p>https://newcmp.sbi/ybPayments/getReqRefencrypt</p> <p>https://newcmp.sbi/ybpayables/payloadUpcoming Pay</p> <p>https://newcmp.sbi/ybPayments/getReqRefdecrypt</p> <p>https://newcmp.sbi/ybPayments/getReqRefencrypt</p> <p>https://newcmp.sbi/ybuseraccess/fetchUserAccesslevel</p> <p>https://newcmp.sbi/ybPayments/getReqRefdecrypt</p> |



| Environment | Environment present/absent (Applicable/ Not Applicable) | Application Name | URL |
|-------------|---|------------------|--|
| | | | <p>https://newcmp.sbi/ybPayments/getReqRefencrypt</p> <p>https://newcmp.sbi/digitalssso/requestRefGenerateReq</p> <p>https://newcmp.sbi/ybPayments/getReqRefdecrypt</p> |
| PROD | Present | SBI FastPlus | <p>https://newcmp.sbi:8443/bulkpaymentapi/cmp/services/</p> <p>https://newcmp.sbi:8443/RealTimeEnquiryServices/Service/Enquiry/</p> <p>https://newcmp.sbi:8443/RealTimePaymentServices/Service/Payment/</p> |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| Environment | Environment present/absent (Applicable/ Not Applicable) | Application Name | URL |
|-------------|---|------------------|--|
| | | | <p>https://newcmp.sbi:8443/SAPPaymentServices/services/SBISoapSrvc?wsdl</p> <p>https://newcmp.sbi:8443/SBIfastplusAPI/mpat/userValidation</p> <p>https://newcmp.sbi:8443/SBIfastplusAPI/mpat/updateTransaction</p> <p>https://newcmp.sbi:8443/SBITokenServices/token/getToken/</p> <p>https://newcmp.sbi/ybPayments/getReqRefencrypt</p> <p>https://newcmp.sbi/ybpending/payloadPendingApprovalTxn</p> <p>https://newcmp.sbi/ybPayments/getReqRefdecrypt</p> |



| Environment | Environment present/absent (Applicable/ Not Applicable) | Application Name | URL |
|-------------|---|------------------|---|
| | | | <p>https://newcmp.sbi/ybPayments/getReqRefencrypt</p> <p>https://newcmp.sbi/ybpayables/payloadUpcoming Pay</p> <p>https://newcmp.sbi/ybPayments/getReqRefdecrypt</p> <p>https://newcmp.sbi/ybPayments/getReqRefencrypt</p> <p>https://newcmp.sbi/ybuseraccess/fetchUserAccesslevel</p> <p>https://newcmp.sbi/ybPayments/getReqRefdecrypt</p> <p>https://newcmp.sbi/ybPayments/getReqRefencrypt</p> |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| Environment | Environment present/absent (Applicable/ Not Applicable) | Application Name | URL |
|-------------|---|------------------|---|
| | | | <p>https://newcmp.sbi/digitalsso/requestRefGenerateReq</p> <p>https://newcmp.sbi/ybPayments/getReqRefdecrypt</p> <p>https://newcmp.onlinesbi.com:8444/SBIGovTokenService/token/getToken</p> <p>https://newcmp.onlinesbi.com:8444/SBIGovIntroService/introService/sendPayLoad</p> <p>https://newcmp.sbi:8443/SbiGovIREPSService/ireps/sendData</p> <p>https://newcmp.sbi:8443/SbiGovIREPSService/ireps/sendMerchantInq</p> <p>https://newcmp.sbi:8443/SbiGovIREPSService/ireps/sendBalanceInq</p> <p>https://newcmp.sbi:8443/ITRO_SBICRM/itrocrm/userdetails</p> <p>https://newcmp.sbi:8444/SBIITDService/ITDService/validatePan</p> <p>https://newcmp.sbi:8444/SBIITDService/ITDService/sendPanAccData</p> |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| Environment | Environment present/absent (Applicable/ Not Applicable) | Application Name | URL |
|-------------|---|------------------|---|
| | | | https://newcmp.sbi:8443/ITRO_SBICRM/itrocrm/getToken |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



CSR 2024-25 Scope Collection Document
Department Name: IT- YB & CINB

1. Application Details

| Sr. No | Name of Application | Criticality rating of application | Type of application (web/mobile /backend process) | Exposed to (Internet/Public NW) | Source Code | | App sec | | No. of web Services/API | Firewall Rules | Vendor Name | Vendor Location |
|--------|----------------------|-----------------------------------|---|---------------------------------|---|-----------------|------------------|----------------------------|-------------------------|---|-------------|-----------------|
| | | | | | LoC (Line of code) | Language | No of user roles | Input pages/ Dynamic pages | | | | |
| 1 | Corporate | High | Web | Internet | 1182784 | Java | 4 | 3690 | 11 | FAR details included in IT-INB Department | TechM | GITC/ Chennai |
| 2 | YONO Business Web | High | Web | Internet | Java – 3,84,000 (approx.) Angular - 107666 (approx.) | AngularJS, Java | 2 | 189 | NA | | TechM | GITC/ Chennai |
| 3 | YONO Business Mobile | High | Mobile | Internet | Approx 100000 | Java & Kony | 2 | Approx 150 | NA | | TechM | GITC/ Chennai |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| Name of Application | No. of Devices for VA/SCD | | | | | |
|----------------------|---------------------------|--------------------|--------------------|--------------------|--------------------|----------------------|
| | OS | DB | App | Web | Others | Total no. of servers |
| | (DC+DR separately) | (DC+DR separately) | (DC+DR separately) | (DC+DR separately) | (DC+DR separately) | (DC+DR separately) |
| Corporate | AIX 7.3, Solaris 11.4 | 3+3 | 6+6 | 4+4 | 5+5 | 18+18 |
| YONO Business Web | AIX 7.3 | 3+3 | 20+20 | 12+12 | 12+12 | 47+47 |
| YONO Business Mobile | AIX 7.3, RHEL 8/9 | 0+0 | 9+9 | 8+8 | 4+4 | 21+21 |

Number of public facing applications: 3

Number of intranet applications: 0

2. Number of 3rd party products (e.g. Radware, Dynatrace etc.):

| Name of 3 rd party product | Name of the vendor | Number of servers in setup | Used for/Purpose |
|---------------------------------------|--------------------|----------------------------|------------------|
|---------------------------------------|--------------------|----------------------------|------------------|

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | |
|--------------------------------|---------|----|--|
| Load Balancer – Alteon 8420 XL | Radware | 18 | For load balancing application traffic |
| ONY version 8.4 | Temenos | 12 | |

3. Number of Merchant Aggregators/Sub-merchants/Direct merchants: NIL

4. Number of new applications added since last CSR (specify name of application as well): NIL

Modules not applicable for CSR: CMP, eTrade and eForex as the appsec review will be part of the respective application owning departments

List of URLs of all the application:

| Application Name | Environment (PROD/UAT) | URL |
|-------------------------|-------------------------------|---|
| YONOB | UAT | https://sityb.sbi |
| YONOB | PROD | https://yonobusiness.sbi |
| Corporate | Preprod | https://corppreprd.onlinesbi.sbi |
| Corporate | UAT / PROD | https://corp.onlinesbi.sbi |
| YONOBUSINESS MOBILE | PROD | https://api.yonobusinessmobile.sbi |
| YONOBUSINESS MOBILE | UAT | https://api.uatyonobusinessmobile.sbi |

We confirm that, all the Existing Applications owned/managed by our department are included in the list and that all the details provided above are correct.



| Sr.No. | Name of Application | Category | Activity | Scope | Deliverables | Scope description |
|--------|---------------------|--------------------------|---|--|---------------|---|
| 1 | SBConnect | Vulnerability assessment | 1. Vulnerability Assessment 2. Penetration testing | 100% coverage of network devices installed at data center (4) and critical Locations (10) and sample devices of other locations 3500 devices including all Data centre devices and critical branches spread across circles. 100% DCDR and sample critical locations Network devices such as: Routers Switches TACACs IDS/IPS Firewalls VPN Devices & End | 1. VA reports | Vulnerability assessment by SOC Team. ISSP to format the raw report shared by SOC team. 3500 devices including all Data centre devices and critical branches spread across circles and FO. |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | |
|--|--|--|--|---|--|--|
| | | | | Points(Sample basis) Web Gateway Scanner Load Balancer The above list is indicative not exhaustive. | | |
|--|--|--|--|---|--|--|



| | | | | | | |
|---|-----------|-----------------------------|---|--|------------------------|--|
| 2 | SBConnect | Secure Configuration review | Secure Configuration Compliance (Routers, Switches, WAVE devices, Firewall) | <p>100% DCDR and sample critical locations Network devices such as: Routers Switches TACACs IDS/IPS Firewalls VPN Devices & End Points(Sample basis) anti DDoS devices Load Balancer The above list is indicative not exhaustive.</p> <p>3500 devices including all Data centre devices and critical branches spread across circles.</p> | SCD complainece review | 1. Configuration review of network devices as per Bank's latest approved SCD document. |
|---|-----------|-----------------------------|---|--|------------------------|--|



| | | | | | | |
|---|-----------|-----------------------------|--|---|---|---|
| 3 | SBConnect | Secure Architecture Review. | <ol style="list-style-type: none"> 1. Network architecture review of datacentre 2. WAN architecture review | <ol style="list-style-type: none"> 1. All Data centers and NOC 2. Review of bank's WAN link 3. Single Point of Failure Analysis for Network between Branch and Data Centres, Sampling based on pairs of service Providers and Nature of Links. | <p>Network architecture review report of all data center devices, segmentation verification such as web, app, db, prod, pre prod, uat etc, and recommendation as per the best practices.</p> <p>Report on SPoF on network between Branch and data centers</p> | <ol style="list-style-type: none"> 1. Security review of Network architecture of the data center, LAN, WAN AND Virtual environment set up for domestic / Foreign Branches. Local HO, etc.. Segmentation verification such as web, app, db, prod, pre prod, uat and recommendations as per the best practices 2. Review placement of firewalls and various zones 3. Network controls in architecture design for communication with third-parties / external networks and within the Bank and the State Bank |
|---|-----------|-----------------------------|--|---|---|---|

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



- group entities
- 4. Data security and Privacy of communication links
- 5. Evaluating Access controls and Authorisation controls
- 6. Evaluating Monitoring controls
- 7. Review of Perimeter security controls
- 8. Risk assessment of critical assets
- 9. Contingency, High Availability, Load balancing, Single Point of failures
- 10. Communication with virtualization setup
- 11. Evaluating scope for enhancing network

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



security of WAN/LAN.

12. Risk assessing Third Party (Extranet) connectives

13. Review of different setup of WAN architecture and traffic flow between Third party service provider, Datacenter and Branches

14. Internet traffic flow analysis

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | |
|---|-----------|-------------------------------|---|---|--|--|
| | SBConnect | | Data leakage review | Data leakage review across Network Infrastructure | Report covering the current setup and proposed controls etc. | Potential Data Leakage points in the Network based on the SNA and process review. |
| 4 | SBConnect | Process and compliance review | Remote Management/VPN access /WebEx and other channels to access Servers, Desktop and Netowrk devices over WAN/Internet | Review of current implementation and controls inline with Cert-In guidelines and best industry practices. | Report on best practices for remote management of servers | Risk assesment of Web ex and current VPN set up including the process of taking VPN connection end to end. |



| | | | | | | |
|--|------------|--|--|---|--|---|
| | SBCconnect | | <p>Review of Bank Practices for Network Management and SLA Review Review of User Access Management, Log monitoring implementation review Incident management process review Process for Signature & Patch Updates and information to all stakeholders Review of DR Plans related to NW Vertical Review of Standard Operational Procedures related to NW Vertical Review of IT & IS Policy Compliance assessment.</p> | <p>With reference to reports submitted by NI and respective SLA's Access control SLA management Devices covered / not covered in monitoring, Level of monitoring, Monitoring process review, Recommendation based on Risk level Process review for signature and patch update and updation of the same to the stakeholders At five DCs, Sample HO and Branches, IT and IS policy compliance review specially against chapters relating to network security.</p> | <p>Review report on Bank's Practices for Network Management and SLA review Report on Log Monitoring Implementation Review Report on Incident management process review Review Report on DR Plans of NW vertical Review report on SOPs of NW vertical Report on Policy compliance Status</p> | <p>Network management process for service providers should include following: 1. Risk Assessment of the network administration process 2. Evaluating Access controls 3. Reviewing SLA management 4. Evaluating Backup and Archival procedures. 5. Evaluating Patch management and change management 6. Risk assessment of log management practices. 7. Evaluating the monitoring controls 8. Evidence verification 9. Risk assessing</p> |
|--|------------|--|--|---|--|---|



| | | | | | | |
|---|-----------|---|---------------------------|--|--|---|
| 5 | SBConnect | Firewall Rulebase review | Firewall rule base review | Firewall rule base review of all firewalls rules implimented for IT_NW&C department applications and SB Connect(Data centre management) managed by IT network department. Process of end to end lifecycle managemnet of Firewall Rules through manual and automated process in detail including the review of SOP for Firewall Rule lifecycle managemnt. | Firewall rule base analysis reports. Detailed report on Firewall rule management (Complete Lifecycle from Rule raised by IT-AO to rule deletion based on various parametres) | Firewall rule base review of Firewall Rules |
| 6 | NAC | 1.Application Security Testing 2.DFRA 3.Network Architecture Review 4.Process Review | | | | NAC Application Review |



| | | | | | | |
|---|-------|--|--|--|--|--------------------------|
| | | 5. Secure Configuration Document 6. VA | | | | |
| 7 | DNS | 1. Application Security Testing 2. DFRA 3. Network Architecture Review 4. Process Review 5. Secure Configuration Document 6. VA | | | | DNS Application Review |
| 8 | Proxy | 1. Application Security Testing 2. DFRA 3. Network Architecture Review 4. Process | | | | Proxy Application Review |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | |
|----|-----|--|--|--|--|------------------------|
| | | Review 5. Secure Configuration Document 6. VA | | | | |
| 9 | VPN | 1. Application Security Testing 2. DFRA 3. Network Architecture Review 4. Process Review 5. Secure Configuration Document 6. VA | | | | VPN Application Review |
| 10 | NTP | 1. Application Security Testing 2. DFRA 3. Network Architecture Review 4. Process Review | | | | NTP Application Review |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | |
|----|-----------|--|--|--|--|-------------------------|
| | | 5. Secure Configuration Document 6. VA | | | | |
| 11 | NSPM | 1. Application Security Testing 2. DFRA 3. Network Architecture Review 4. Process Review 5. Secure Configuration Document 6. VA | | | | NSPM Application Review |
| 12 | NOC Tools | | | | | |
| | | | | | | |



| | | | | |
|------|----------------------|--|--|-------------------|
| 12.1 | NPMD | <p>1.Application Security Testing</p> <p>2.DFRA</p> <p>3.Network Architecture Review</p> <p>4.Process Review</p> <p>5.Secure Configuration Document</p> <p>6. VA</p> | <p>1.URL : https://npmd.noc.sbi/</p> <p>2.Total Assets</p> <p>a.Web Server: 4 OS : Custom OS RHEL/Ubuntu</p> <p>b.APP Server: 62 OS: Windows/ RHEL / Cutom OS</p> <p>3.Total Number of Roles : 3 (Admin/User/Central manager R&W)</p> <p>4..Appliances: Cubro 4 OS / Linux</p> | NPMD Tool Review |
| 12.2 | Vunet - VuSmart Maps | <p>1.Application Security Testing</p> <p>2.DFRA</p> <p>3.Network Architecture Review</p> <p>4.Process Review</p> <p>5.Secure Configuration Document</p> <p>6. VA</p> | <p>1.URL : https://noc.sbi/</p> <p>2.Total Assets</p> <p>a.Web Server: 5 OS : Ubuntu</p> <p>a.APP Server: 28 OS: Ubuntu</p> <p>b.DB Server: 13 OS : Ubuntu</p> <p>3.Total Number of Roles : 3 (Admin/User/Central manager R&W)</p> | Vunet Tool Review |
| | | | | |



| | | | | | | |
|------|-------------------|---|--|--|--|-----------------------------|
| 12.3 | BMC Remedy (ITSM) | <ol style="list-style-type: none"> 1.Application Security Testing 2.DFRA 3.Network Architecture Review 4.Process Review 5.Secure Configuration Document 6. VA | | <ol style="list-style-type: none"> 1.URL : https://itsm-smartit.noc.sbi/ 2.Total Assets <ol style="list-style-type: none"> a.Web Server: 20 OS : Windows / RHEL a.APP Server: 12 OS: Windows b.DB Server: 4 OS : Windows 3.Total Number of Roles : 3 (Admin/User/Central manager R&W) | | BMC Remedy Tool Review |
| 12.4 | Automation Edge | <ol style="list-style-type: none"> 1.Application Security Testing 2.DFRA 3.Network Architecture Review 4.Process Review 5.Secure Configuration Document 6. VA | | <ol style="list-style-type: none"> 1.URL : https://rpa.noc.sbi/ 2.Total Assets <ol style="list-style-type: none"> a.Web Server: 4 OS : Windows a.APP Server: 10 OS: Windows b.DB Server: 2 OS : Windows 3.Total Number of Roles : 3 (Admin/User/Central manager R&W) | | Automation Edge Tool Review |



| | | | | | | |
|------|----------------------|---|--|--|--|----------------------------------|
| 12.5 | TCP Wave | <ul style="list-style-type: none"> 1.Application Security Testing 2.DFRA 3.Network Architecture Review 4.Process Review 5.Secure Configuration Document 6. VA | | <ul style="list-style-type: none"> 1.URL : NA 2.Total Assets <ul style="list-style-type: none"> a.Web Server: NA a.APP Server: 4 OS: TCPwave-IPAM-5.13 b.DB Server: NA 3.Total Number of Roles : 3 (Admin/User/Central manager R&W) | | TCP Wave Tool Review |
| 12.6 | Avaya Contact Centre | <ul style="list-style-type: none"> 1.Application Security Testing 2.DFRA 3.Network Architecture Review 4.Process Review 5.Secure Configuration Document 6. VA | | <ul style="list-style-type: none"> 1.URL : NA 2.Total Assets <ul style="list-style-type: none"> a.Web Server: NA a.APP Server: 45 OS: RHEL b.DB Server: 6 OS :MS-SQL 3.Total Number of Roles : 3 (Admin/User/Central manager R&W) | | Avaya Contact Centre Tool Review |



CSR 2024-25– Scope collection document

Name of the Department: IT PE-I

| S/N | Name of Application | Submodules Name | Type of application (web/mobile/backed processes) | Exposed to (Internet/Public/NW) | No. of Devices for VA/SCD | | | | | | Firewall rules count | Source Code | | Appsec | | No. of web Services | No. of APIs |
|-----|---------------------|---|---|---------------------------------|---|----|-----|-----|--------|-------|----------------------|-------------|----------|------------------|---------------------------|---------------------|-------------|
| | | | | | OS | DB | App | Web | Others | Total | | LoC | Language | No of user roles | Input pages/Dynamic pages | | |
| 1 | ADS | SFTP Server, KMS, AD User Management Portal, CA Server, AD Password | Infra | No | 162(Windows Server 2016/Windows Server 2019 | 1 | 160 | 1 | 0 | 162 | 5 | NA | NA | 1 | 1 | NA | NA |



| | | | | | | | | | | | | | | | | | |
|---|-------------------------------|---|-----------------|----------|----------------------|----|----|---|---|---------|----|----|----|-------|----|----|----|
| | | Protection Server | | | | | | | | | | | | | | | |
| 2 | AVS | Apex Central, Deep Security, ACC-FIM, EDR | Backend | No | 108 - Windows Server | 36 | 72 | 0 | 54 Non-Windows (40- service gateway, 10- Ind-SPS, 4 - DDAN) | 16 2 | 14 | NA | NA | Admin | NA | 0 | 0 |
| 3 | Patch management System (PMS) | WSUS | | Intranet | 6 | 3 | 3 | 0 | 0 | 6 | 8 | NA | NA | NA | NA | NA | NA |
| | | MECM | | Intranet | 17 | 4 | 13 | 0 | 0 | 17 | 7 | NA | NA | NA | NA | NA | NA |
| 4 | SSO | Single Sign On (SSO) | Backend Process | Intranet | 10 | 4 | 6 | 0 | 0 | 10 | 5 | NA | NA | Admin | NA | 0 | 0 |

Third Party / Vendors where Sensitive data flows outside Bank

| Name Integration of the Third Party/Vendor | Location | Services offered / Purpose of |
|--|---------------------|--------------------------------|
| AWS Cloud (EDR) | GPX-Andheri, Mumbai | Trend Micro Vision One Console |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



Microsoft

Pune, Chennai, Mumbai

Office 365 productivity and security suite on SAAS model



CSR 2024-25– Scope collection document
Name of the Department: IT – Cloud Solutions

| S/ N | Name of Application | Submodules Name | Type of application (web/mobile /backend processes) | Exposed to (Internet/Public/NW) | No. of Devices for VA/SCD | | | | | Total | Fire wall rule s count | Source Code | | Appsec | | No. of web Services | N o. of A PI |
|---------|---------------------|-----------------|---|---------------------------------|---------------------------|-----|-------|------|---------|-------|------------------------|-------------|-----------|------------------|---------------------------|---------------------|--------------|
| | | | | | O S | D B | A p p | W eb | Oth ers | | | Lo C | Lang uage | No of user roles | Input pages/Dynamic pages | | |
| | | | | | | | | | | | | | | | | | |



| | | | | | | | | | | | | | |
|---|-------------------------|---|----------------------------|------------------------------|------------------------------------|------|----|----|----|------------|----|----|----|
| 1 | Meghdoot Infrastructure | <p>VMware VCF</p> <ol style="list-style-type: none"> 1. VMware ESXi 2. NSX 3. vCenter 4. SDDC Manager 5. SRM (Site Recovery Manager) 6. Aria Operations (vROPS) 7. Aria Automation (vRA) 8. Aria Operations for Logs(vRLI) 9. AVI Vantage Advance Load | Infrastructure Application | No. Only Intranet accessible | App – 117 OS-954 (Esxi, Jump host) | 1071 | 26 | NA | NA | L1, L2, L3 | NA | NA | NA |
|---|-------------------------|---|----------------------------|------------------------------|------------------------------------|------|----|----|----|------------|----|----|----|



| | | | | | | | | | | | | | |
|---|-------------------------------|---|---------------------------------------|------------------------------------|---|---------|----|--------|----|--------------|----|----|--------|
| | | Balancer 10.VMware Aria Operations for Networks 11.vRealize Lifecycle Manager | | | | | | | | | | | |
| 2 | Meghdot Infrastr ucture | VMware Tanzu | Hosts & Applian ces | No. Only Intranet accessible | APP – 774 | 77 4 | 11 | N A | NA | L1,L 2,L3 | NA | NA | N A |
| 3 | | Enterprise Backup Solution (EBS) - Commserv er - Mediaagent | Infrastr ucture Applicat ion | No. Only Intranet accessible | APP-24 (Media Agent) DB – 4 (Commserve Web console) | 28 | 6 | N A | NA | L1,L 2,L3 | NA | NA | N A |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | | | | | | | | |
|---|----------------|--|----------------------------|------------------------------|--|-----|----|----|----|----------|----|----|----|
| | | s - Webserver - webconsole | | | | | | | | | | | |
| 4 | NetApp Storage | Console & File system Configurations | Infrastructure Application | No. Only Intranet accessible | Others – 140 (Nodes, SAN Switch, Cluster, Switch, NA Box, Monitoring Tool) | 140 | 11 | NA | NA | L1,L2,L3 | NA | NA | NA |



CSR 2024-25 – Scope Collection Document
Name of the Department: Data Centres & Operations

| S/N | Name of Application | Submodules Name | Type of application (web/mobile /backend process) | Exposed to (Internet/Public/NW) | No. of Devices for VA/SCD | | | | | | Firewall rules count | Source Code | | Appsec | | No. of web Services | | No. of API |
|-----|--------------------------|-----------------|---|---------------------------------|---------------------------|----|-----|-----|--------|-------|----------------------|-------------|----------|------------------|----------------------------|---------------------|--|------------|
| | | | | | OS | DB | App | Web | Others | Total | | LoC | Language | No of user roles | Input pages /Dynamic pages | | | |
| 1 | GITC DC, Belapur | NIL | NA | NA | | | | | | | | NA | | | | | | |
| 2 | Sify DC, Rabale | NIL | NA | NA | | | | | | | | NA | | | | | | |
| 3 | Gachibowli DC, Hyderabad | NIL | NA | NA | | | | | | | | NA | | | | | | |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | |
|---|-------------------------------|-----|----|----|----|
| 4 | CtrlS DC, Hydera bad | NIL | NA | NA | NA |
|---|-------------------------------|-----|----|----|----|



SCOPE FY 2024-25

NAME OF THE DEPARTMENT: IT Special Projects – II

| S r | Name of Applicat ion/ Compon ents | Date of initiati on of last review | Applicat ion hosted on or off premise | No. of Devices for VA/SCD | | | | | Source Code (Whether Audit Right available with Bank or not) | Appsec | | No of A PI | SNA Revi ew | Proc ess Revi ew | End to End DF D | |
|--------|---|--|--|------------------------------|--------|---------|---------|-----------|---|------------------|------------------------|---------------------|-------------------|---------------------------|-----------------------------|---------------------|
| | | | | OS | D B | Ap p | W eb | Tot al | | LoC (approx.) | Langua ge | | | | | Privileg e Level |
| 1 | AMLOC K TM | 17-07- 2023 | On premise (Physica l hardwar e) | 12 | 4 | 4 | 4 | 12 | No. Source Code maintaine d by M/s Azentio. | Java / Oracle | Appuse r/ Oracle | 133 | 0 | Yes | Yes | Yes |
| 2 | AMLOC K ESS | 17-07- 2023 | | 12 | 4 | 4 | 4 | 12 | | Java / Oracle | Appuse r/ Oracle | 27 | 1 | Yes | Yes | Yes |
| 3 | AMLOC K TFSS | 17-07- 2023 | | 12 | 4 | 4 | 4 | 12 | | Java / Oracle | Appuse r/ Oracle | 21 | 1 | Yes | Yes | Yes |
| 4 | AMLOC K RMS | 17-07- 2023 | | 12 | 4 | 4 | 4 | 12 | | Java / Oracle | Appuse r/ Oracle | 59 | 0 | Yes | Yes | Yes |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| Sr | Name of Application/ Components | Date of initiation of last review | Application hosted on or off premise | No. of Devices for VA/SCD | | | | | Source Code (Whether Audit Right available with Bank or not) | | Appsec | | No. of API | SNA Review | Process Review | End to End DFD |
|----|---------------------------------|-----------------------------------|--------------------------------------|---------------------------|----|-----|-----|-------|--|---------------|-----------------|----------------------------|------------|------------|----------------|----------------|
| | | | | OS | DB | App | Web | Total | LoC (approx.) | Language | Privilege Level | Input pages/ Dynamic pages | | | | |
| 5 | AMLOCK OTSS | 17-07-2023 | | 12 | 4 | 4 | 4 | 12 | | Java / Oracle | Appuser/ Oracle | 30 | 1 | Yes | Yes | Yes |
| 6 | AMLOCK OSTR | - | | 14 | 4 | 4 | 6 | 14 | 3000 | .Net | Appuser/ Oracle | 20 | 3 | Yes | Yes | Yes |
| 7 | AMLCFT CONNECT | 17-07-2023 | | 4 | 2 | 2 | 0 | 4 | 22203 | .Net | Appuser/ Oracle | 20 | 0 | Yes | Yes | Yes |
| 8 | APY | 15-06-2022 | Meghdoot | 8 | 2 | 5 | 3 | 8 | 68000 | Java | Maker/ Checker | Dynamic Pages | 4 | Yes | Yes | Yes |
| 9 | NPS | 15-06-2022 | Meghdoot | 11 | 3 | 7 | 3 | 11 | 1.51 Lacs | Java | Maker/ Checker | Dynamic Pages | 20 | Yes | Yes | Yes |



| Sr | Name of Application/ Components | Date of initiation of last review | Application hosted on or off premise | No. of Devices for VA/SCD | | | | | Source Code (Whether Audit Right available with Bank or not) | | Appsec | | No. of API | SNA Review | Process Review | End to End DF D |
|----|---------------------------------|-----------------------------------|--------------------------------------|---------------------------|------|----------------|--------------|----------------|--|-------------------|---|----------------------------|------------|------------|----------------|-----------------|
| | | | | OS | DB | App | Web | Total | LoC (approx.) | Language | Privilege Level | Input pages/ Dynamic pages | | | | |
| 10 | GCC | 15-06-2022 | Meghdot | 9 | 1 | 6 | 2 | 9 | 122500 | Java | Maker/Checker | Dynamic Pages | 2 | Yes | Yes | Yes |
| 11 | GRC | 15-06-2022 | Meghdot | 2 | 1 | 1 | 0 | 2 | 48209 | Java | UCO,LHO,Branch | Dynamic Pages | 6 | Yes | Yes | Yes |
| 12 | OSMP | 15-06-2022 | Meghdot | 5 | 2 | 1 | 2 | 5 | 53000 | .net, C#, Angular | Maker, Checker, CnSD Admin, LHO/RSD Admin | 10 | NA | Yes | Yes | Yes |
| 13 | iFAMS | 15-06-2022 | Meghdot | 15 PR 15 DR | 3 PR | 10 PR 10 DR | 2 PR 2 DR | 15 PR 15 DR | 2 lacs | Oracle ADF | Maker/Checker | Dynamic | 2 | Yes | Yes | Yes |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| Sr | Name of Application/ Components | Date of initiation of last review | Application hosted on or off premise | No. of Devices for VA/SCD | | | | | Source Code (Whether Audit Right available with Bank or not) | | Appsec | | No. of API | SNA Review | Process Review | End to End DFD |
|----|---------------------------------|-----------------------------------|--------------------------------------|---------------------------|--------|---------|--------|------------------------------|--|-------------------|----------------------|----------------------------|------------|------------|----------------|----------------|
| | | | | OS | DB | App | Web | Total | LoC (approx.) | Language | Privilege Level | Input pages/ Dynamic pages | | | | |
| | | | | | 3 | | | | | | | | | | | |
| 14 | OARPS | 15-06-2022 | Meghdot | 14 13 | 2 2 | 10 9 | 2 2 | 14 PR 13 DR | 12 Lacs | Java (Spring MVC) | Maker/Checker/SSY/SY | 800 | 10 | Yes | Yes | Yes |
| 15 | RADAR | 15-06-2022 | Meghdot | 4 4 | 1 1 | 2 2 | 1 1 | 4 PR 4 DR (passive) | 2.20 Lakhs | Java/Angular | Maker/Checker | 30 | 8 | Yes | Yes | Yes |
| 16 | RFCA | 15-06-2022 | Meghdot | 4 4 | 1 1 | 2 2 | 1 1 | 4 PR 4 DR | 5.3 lakhs | C# | Maker/Checker/Admin | 450 | 5 | Yes | Yes | Yes |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| Sr | Name of Application/ Components | Date of initiation of last review | Application hosted on or off premise | No. of Devices for VA/SCD | | | | | Source Code (Whether Audit Right available with Bank or not) | | Appsec | | No. of A PI | SNA Review | Process Review | End to End DF D |
|----|---------------------------------|-----------------------------------|--------------------------------------|---------------------------|----|-----|-----|-----------|--|----------|-----------------|----------------------------|-------------|------------|----------------|-----------------|
| | | | | OS | DB | App | Web | Total | LoC (approx.) | Language | Privilege Level | Input pages/ Dynamic pages | | | | |
| | | | | | | | | (passive) | | | | | | | | |

Review includes Forensic readiness and Threat intelligence.
 External URLs, If any: None



CSR 2024-25 — Scope collection document
IT-YONO

| S.No | Name of Application | Submodule Name/Component list | Type of application (web/mobile/backend process) | Exposed to (Internet/Public NW) | No. of Devices for VA/SCD | | | | | |
|------|---|---|--|---------------------------------|--|-----|-----|-----|---|-------|
| | | | | | os | Web | App | DB | Others (Appliance/Special devices) | Total |
| 1 | IT-YONO (All components supporting YONO by SBI Application) | MFP,IIB,WAS,SPS S,Unica,Datastage,Cloudant,DB2 Filenet,TWS, IBM Spectrum Protect,Cognos, Magento,Kafka, ELK,Elastic Search,API, Continuity Petrol, WAF etc. | Mobile and Branch portal. | Yes | Production (App+Web+DB) AIX-410 RHEL-221 | 47 | 480 | 104 | 347 | 978 |
| | | | | | | | | | Component wise breakup: Custom/Special Appliance: 4 NPS and 124 APIC, Virtualization related infra: 10 Windows, 4 Vcenter, 25 HyperV, 2 PowerVC, 92 Esxi Security related | |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|---|--|
| | | | | | | | | | | appliances: 19 WAF & LB, 6 BIG IQ Storage related infra: 4 Tape Library, 57 SAN Switch, SVC and Storage | |
|--|--|--|--|--|--|--|--|--|--|---|--|



CSR 2024-25 : SCOPE COLLECTION DOCUMENT

Name of the Department -IT-YONO

| S.No | Name of the Application | Sub Module Name | Type of Application (web/mobile/backend/process) | Exposed to Internet/Public NW | No. of Devices for VA/SCD | | | | Language | APPSEC | | No. of API/Webservices | | | |
|------|-------------------------|-----------------|--|-------------------------------|---------------------------|---|---|---|--------------|-----------------------------------|-----------------|------------------------|-----------------------------|----------|----------|
| | | | | | C | D | A | W | | LO | No. of Journeys | No. of User Roles | No. of Input /Dynamic Pages | Internal | External |
| 1 | YONO -All comp | YONO - Mobile | Mobile | Internet | 1 | N | N | N | 10, 10, 50 0 | JavaScript,HTML,JAVA,eSQL,SQL,PHP | 135 | 1 | 1000 | 4 | 15 |

Engaging CAT-I Competent ISSPs from GIRC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | | | | | | | | | |
|---|--------------------------|---------|--------------|--|--------|--------|--------|-----------------------|---|----|---|-----|--|--|
| on ent s sup por ting YO NO by SBI App licat ion) | Bra nch Por tal | We b | Intern et | | N A | N A | N A | 11, 70, 00 0 | JavaScript,H TML,JAVA,e SQL,SQL,PH P | 14 | 2 | 500 | | |
|---|--------------------------|---------|--------------|--|--------|--------|--------|-----------------------|---|----|---|-----|--|--|



CSR 2024-25– Scope collection document
Department Name: Core Banking Development

| S/ N | Name of Application | Submodule Name | Type of application (web/mobile /backend process) | Criticality | Exposed to (Internet / Public NW) | No. of Devices for VA/SCD | | | | | Source Code | | App sec | | No. of web Services | No. Of Firewall Rules | No. of API |
|------|---------------------|--|---|-------------|-----------------------------------|---------------------------|----------|----------|----------|----------|-------------|--|------------------|----------------------------|---------------------|-----------------------|------------|
| | | | | | | OS | DB | App | Web | Total | LoC | Language | No of user roles | Input pages/ Dynamic pages | | | |
| 1 | CBS | Frontend, Interface, Loans, Deposit, CIF, NDVP, GL | Web application | High | No | CBT O | CBT O | CBT O | CBT O | CBT O | 2cr+ | Cobol, .NET, Shell, PERL, VB.Net, HTML, JavaScript | 30 | 6000 approx. | 15 | CBTO | CBTO |
| 2 | ADV | Admin Module | Web application | Medium | No | CBT O | CBT O | CBT O | NA | CBT O | 72000 | Java | 2 | Dynamic (5) | NA | CBTO | NA |
| | ADV | Batch Module | Backend process | | No | CBT O | CBT O | CBT O | NA | CBT O | 8000 | Java | NA | NA | NA | CBTO | NA |
| | ADV | API module | Web application | | No | CBT O | CBT O | CBT O | CBT O | CBT O | 25000 | Java | NA | NA | NA | CBTO | 4 |
| | ADV | Tokenization Module | Backend process | | No | CBT O | CBT O | CBT O | NA | CBT O | 38003 | Java | NA | NA | NA | CBTO | NA |
| 3 | CBS-NE | N/A | Web & Backend | Medium | No | CBT O | CBT O | CBT O | CBT O | CBT O | 62000+ | JAVA | 2 | 14 | NA | 5+ UAT | NA |



| | | | | | | | | | | | | | | | | | FARs, Production FAR's maintained by Tech Ops | |
|---|---------------------|-----|---------|--------------|----------|------|----|------|----|------|---------|------------|----|------|----|-----|---|--|
| 4 | CCDP | N/A | Web | Medium | Intranet | 36 | 0 | 12 | 24 | 36 | 1.90 L~ | C#, PL/SQL | 4 | 160+ | 0 | 30+ | 3 | |
| 5 | SDM | NA | Web | Low | No | 4 | 1 | 2 | 1 | 4 | 130000+ | JAVA | 13 | 42 | 1 | 23 | NA | |
| 6 | Distributor | NA | Backend | Low | No | CBTO | NA | CBTO | NA | CBTO | 16000+ | C | 3 | NA | NA | 6 | NA | |
| 7 | IR Tracking | NA | Web | Low | No | 1 | NA | 1 | NA | 1 | 45000+ | CGI | NA | NA | 1 | 5 | NA | |
| 8 | CBDEV Portal | N/A | Web | Non-critical | Intranet | 1 | NA | NA | 1 | 1 | 2000~ | C# | 1 | None | 0 | 1+ | 0 | |

Count of External Facing IPs: 0
 Count of other Appliances (LB, DPG etc.): NA



CSR 2024-25 : Scope Collection Document
Department Name: CB-Tech-Operations

| S/N | Name of Application | Criticality | Submodule Name | Type of application (web/mobile /backend process) | Exposed to (Internet / Public NW) | No. of Devices for VA/SCD | | | | | Source Code | | App sec | | No. of web Services | No. Of Firewall Rules | No. of API |
|-----|---------------------|-------------|----------------|---|------------------------------------|---|--------------------------------------|---------------------------------------|----------------------------------|------------|-------------|----------|------------------|----------------------------|---------------------|-----------------------|------------|
| | | | | | | OS | DB | App | Web | Total | LoC | Language | No of user roles | Input pages/ Dynamic pages | | | |
| 1 | CBS | High | CBS | Backend | No | HPUX-168 PR-56 DR-54 NR- 58 RHEL- 8 (PR-4 NR-2 DR-2) Win -19 (PR-12 DR-7) Total - 195 | 82 PR-30 DR-22 NR-30 | 113 PR-42 DR-41 NR-30 | 6 PR-2 DR-2 NR-2 | 195 | NA | NA | NA | NA | NA | 158 | Nil |
| 2 | Hadoop | Low | Hadoop | Backend Process | No | 26 PR – 13 DR – 13 | PR-1 DR-1 | PR-1 DR-1 | | 26 | 9150 | Java | 7 | 4 | NIL | 21 | NIL |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | | | | | | | | | | | | |
|---|---------------------|--------|---------------|--|----|-----------------------|-----------------------|----------------------|-----------------------|----|-----------------|-----------------|--------------|--------------|----|----|-----|
| 3 | IPM+ | Low | IPM+ | Infrastructure Mgmt. and Backend Processes | NA | 2 PR – 1 DR – 1 | 2 PR – 1 DR – 1 | 2 | 2 PR – 1 DR – 1 | 2 | NA - Outsourced | NA - Outsourced | No Front end | No Front end | 1 | 8 | NIL |
| 4 | Notification Engine | Low | NE(CBS -Lite) | NE Backend Application Process | No | 38 PR-19 DR-19 | 2 PR-1 DR-1 | 32 PR-16 DR-16 | 4 PR-2 DR-2 | 38 | NA | NA | 2 | AO is CB-DEV | 2 | 19 | 1 |
| 5 | BSC | Medium | BSC | Infrastructure Project | No | As per Annexure-A | | | | | NA | NA | NA | NA | NA | 21 | NA |

Count of External Facing IPs: Nil

Details of third party:

| Name of the Third Party/ Vendor | Location | Services offered / Purpose of Integration | Supply Chain Control Point Report Available / To be Reviewed |
|------------------------------------|------------|---|---|
| TCS | On premise | Operation Support | |
| NTT | On premise | Operation Support | |

* CBS Infrastructure includes the infrastructure related to Golden Gate, Finance One, CCDP and Distributor.



Annexure A

| PR | | | DR | | | Status of DC DR |
|---------------------|-------------|----------------|--------------|----------|-------------|-----------------|
| Components | OS(VA) | DB | OS | DB | Total (SCD) | |
| Branch Server | 208 | | 208(Passive) | 0 | 416 | Active-Passive |
| RDSH | 10 | Active-Passive | 10 | 0 | 20 | Active-Active |
| Management Server | 247 | Active-Active | 223 | 4 | 470 | |
| Vmware Esxi | 521 | 0 | 525 | 0 | 1,046 | |
| Cisco Nexus 9K | 12 | 0 | 12 | 0 | 24 | |
| Cisco Nexus 5K | 2 | 0 | 2 | 0 | 4 | |
| Cisco Nexus 3K | 10 | 0 | 10 | 0 | 20 | |
| Cisco MDS | 10 | 0 | 10 | 0 | 20 | Active-Passive |
| Avamar Backup M1200 | 10 | 0 | 10 | 0 | 20 | |
| EMC Data Domain | 5 | Active-Passive | 5 | 0 | 10 | Active-Active |
| VNXe 3200 | 5 | 0 | 5 | 0 | 10 | |
| Total | 1040 | 6 | 1020 | 4 | 2070 | |



CSR 2024-25 Scope collection document
Department Name: New Branch Channel Department

| S/N | Name of Application | Submodule Name | Criticality | Type of application (web/mobile /backend process) | Exposed to (Internet/ Public NW) | No. of Devices for VA/SCD – DC & DR | | | | | | Source Code | | App sec | | No. of web Services | No. Of Firewall Rules | No. of API |
|-----|---------------------|----------------|-------------|---|----------------------------------|-------------------------------------|-----|------|------|---------------|--------|-------------|-----------|--------------------|-----------------------------|---------------------|-----------------------|------------|
| | | | | | | O S | D B | Ap p | We b | Ma nag em ent | Tot al | LoC | Lang uage | No of use r role s | Input pages/ Dyna mic pages | | | |
| 1 | New Branch Channel | | HIGH | Web | Intranet | REL 8.9 (23+) window server | 55 | 1010 | 6+ | 5+5 | 26+26 | 6Lac+ | JAVA | 30 | 440 | NA | | NA |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | | | | | | | | | | | | | | | |
|--|--|--|--|--|--|--|---------------------------------|--|--|--|--|--|--|--|--|--|--|--|--|--|
| | | | | | | | er 20 19 (1 +1) | | | | | | | | | | | | | |
|--|--|--|--|--|--|--|---------------------------------|--|--|--|--|--|--|--|--|--|--|--|--|--|

NBC Production Servers are with CB Tech-OPS so ownership is with CBTechOps for scope of review for INFRA and related activities. Application ownerships is with NBC Dept. Please refer the Annexure below for various scope activities.

Count of External Facing IPs: **NA**

Count of other Appliances (LB, DPG etc.): NA

Details of Third Party : NA

| Name Integration of third party/vendor | Location | Services offered/Purpose of | 43 point control report available/to be reviewed |
|--|----------|-----------------------------|--|
| | | | |
| | | | |

ANNEXURE :

| Application name | Ownership department name for activity | | | | | | | | | | |
|------------------|--|------------|--------------------|------|------|------|------------|------|------------------|--------------------|-------------------------|
| | Appsec | API review | Source code review | VA | SCD | SNA | FAR review | DFRA | DB review | Process review/DFD | 3rd party vendor review |
| NBC | NBC | NA | NBC | CBTO | CBTO | CBTO | CBTO | CBTO | CBTO/NBC | NBC | NA |
| | | | | | | | | | Refer Note Below | | |
| | | | | | | | | | | | |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



Note for Detailed Activities :

DB Review - NBC / CB- TechOps. Review related to DB maintenance activities for DB engine will be done by CBTO. NBC will look after the review details for the database design, schema and the content of the database including masking, data encryption etc.

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



CSR scope for FY 2024-25
Department Name: IT- Retail Loans

RAAS

| S/N | Name of Application | Submodule Name | Type of application (web/mobile /backend process) | Application Criticality | Exposed to (Internet/Public NW) | No. of Devices for VA/SCD | | | | | | Source Code | | App sec | | No. of web Services | No. Of Firewall Rules | No. of API |
|-----|---------------------|----------------|---|-------------------------|---------------------------------|---------------------------|----|-----|-----|--------|-------|-------------|----------|------------------------------------|----------------------------|---------------------|-----------------------|------------|
| | | | | | | OS | DB | App | Web | Others | Total | LoC | Language | No of user roles/ Privilege levels | Input pages/ Dynamic pages | | | |
| 1 | RAAS | RAAS | Web Application | Medium | No | 6 | 2 | 2 | 2 | 0 | 6 | 300000 | .Net | NA | 20/100 | 0 | 60 | 8 |

Whether all previous CSR closed? **Yes**

Count of External Facing IPs: **Nil**

Count of other Appliances (LB, DPG etc.): **Nil**

Details of third party: **NA**

LAMS

| S / N | Name of Application | Criticality | Submodule Name | Type of application (web/mobile /backend process) | Exposed to (Internet/Public NW) | No. of Devices for VA/SCD | | | | | Source Code | | App sec | | No. of web Services | No. Of Firewall Rules | No. of API |
|-------|---------------------|-------------|----------------|---|---------------------------------|---------------------------|----|-----|-----|-------|-------------|----------|------------------|----------------------------|---------------------|-----------------------|------------|
| | | | | | | OS | DB | App | Web | Total | LoC | Language | No of user roles | Input pages/ Dynamic pages | | | |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | | | | | | | | | | | |
|---|-------|--------|-----|----|----|---|---|---|----|-------|------|----|----|------------------------|----|-----------------|
| 1 | LAM S | Medium | Web | No | 12 | 4 | 4 | 4 | 12 | 50000 | .NET | 12 | 35 | 1 agent authentication | 60 | 3 EIS, sms, crm |
|---|-------|--------|-----|----|----|---|---|---|----|-------|------|----|----|------------------------|----|-----------------|

Whether all previous CSR closed? **Yes**

Count of External Facing IPs: 0

Count of other Appliances (LB, DPG etc.): 0

Details of Third Party: NA

VVM

| S / N | Name of Application | Submodule Name | Type of application (web/mobile /backend process) | Application Criticality | Exposed to (Internet/Public NW) | No. of Devices for VA/SCD | | | | | Source Code | | App sec | | No. of web Services | No. Of Firewall Rules | No. of API |
|-------|---------------------|----------------|---|-------------------------|----------------------------------|---------------------------|----|-----|-----|--------|-------------|-----|----------|-----------------------------------|---------------------|-----------------------|------------|
| | | | | | | OS | DB | App | Web | Others | Total | LoC | Language | No of user roles/Privilege levels | | | |
| | | | | | | | | | | | | | | | | | |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | | | | | | | | | | | | | |
|---|-----|--|--------|--------|-----|----|---|---|---|---|----|------------|------|---|----|---|----|---|
| 1 | VVM | https://lmsv vm.stateban ktimes.in/V VM/internal/ login | Web | Medium | No | 16 | 4 | 4 | 8 | 3 | 35 | 54607 6 | Java | 2 | 13 | 0 | 30 | 1 |
| 2 | VVM | https://vvm. bank.sbi:944 5/VVM/port al/login | Web | Medium | Yes | | | | | | | | Java | 3 | 12 | 0 | | 1 |
| 3 | VVM | SIO Mobile Android Application placed in Intune private App | Mobile | Medium | Yes | | | | | | | | Java | 1 | 9 | 0 | | 6 |

Whether all previous CSR closed? **Yes**
 Count of External Facing IPs: **1**
 Count of other Appliances (LB, DPG etc.): **NA**
 Details of third party: **NA**



RLMS

| S / N | Name of Application | Submodule Name | Type of application (web/mobile/backend process) | Application Criticality | Exposed to (Internet/Public NW) | No. of Devices for VA/SCD | | | | | Source Code | | App sec | | No. of web Services | No. Of Firewall Rules | No. of API |
|-------|---------------------|----------------|--|-------------------------|---------------------------------|---------------------------|----|-----|-----|-------|-------------|----------|------------------|---------------------------|---------------------|-----------------------|------------|
| | | | | | | OS | DB | App | Web | Total | LoC | Language | No of user roles | Input pages/Dynamic pages | | | |
| 1 | RLMS | Gateway | API | Medium | NO | 38 | 2 | 28 | 8 | 76 | ~28220 | Java | 45 | NA | 390 | 250+ | 638 |
| 2 | | Common API | API | | NO | | | | | | ~189708 | Java | | NA | 96 | | 96 |
| 3 | | GP API | API | | NO | | | | | | ~35970 | Java | | NA | 79 | | 79 |
| 4 | | XP API | API | | NO | | | | | | ~30551 | Java | | NA | 86 | | 86 |
| 5 | | EXT API | API | | NO | | | | | | ~23095 | Java | | NA | 61 | | 61 |
| 6 | | RLMS INT | API | | NO | | | | | | ~74030 | Java | | NA | 68 | | 68 |
| 7 | | ADMIN | API | | NO | | | | | | ~14672 | Java | | NA | 114 | | 114 |
| 8 | | HL API | API | | NO | | | | | | ~30845 | Java | | NA | 135 | | 135 |
| 9 | | HLRP API | API | | No | | | | | | ~30545 | Java | | NA | 106 | | 106 |
| 10 | | AL API | API | | NO | | | | | | ~18762 | Java | | NA | 60 | | 60 |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | | | | | | | | | | | |
|---|--|-----|-----|--|----|--|--|--|--|--------|------------|--|-------|-------|--|-------|
| 1 | | LAS | API | | NO | | | | | ~5893 | Java | | NA | 16 | | 16 |
| 1 | | API | | | | | | | | | | | | | | |
| 1 | | UI | WEB | | NO | | | | | 5Lacks | Typescript | | ~1500 | ~1200 | | ~1000 |
| 2 | | | | | | | | | | | | | | | | |

Whether all previous CSR closed? **Yes**
 Count of External Facing IPs: 0
 Count of other Appliances (LB, DPG etc.): 0
 Details of Third Party: NA

Details of third party

| Name of the Third Party/ Vendor | Location | Services offered / Purpose of Integration | Supply Chain Control Point Report Available / To be Reviewed |
|---------------------------------|--------------|---|--|
| Tech Mahindra | GITC Belapur | Support, Maintenance and Development of OCAS application. | Not Available |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



CSR 2024-25 – Scope collection document

Department Name: IT-Agri Tech

| Sr No | Name of Application | Sub module Name | Type of application (web/mobile/backend process) | Application Criticality | Exposed to (Internet/Public NW) | No. of Devices for VA/SCD | | | | | | Source Code | | App sec | | No. of web Services | No. Of Firewall Rules | No. of API |
|-------|---------------------|-----------------|--|-------------------------|----------------------------------|---------------------------|----|-----|-----|--------|-------|----------------|-------|-----------------------------------|---------------------------|---------------------|-----------------------|------------|
| | | | | | | OS | DB | App | Web | Others | Total | LoC | Lang. | No of user roles/Privilege levels | Input pages/Dynamic pages | | | |
| 1 | AGRI LMS | | Web | Medium | Intranet | 80 | 14 | 54 | 12 | 0 | 80 | 51890 (approx) | JAVA | 10 | 24 (work steps) | NA | 90 | 0 |

| | LOS Agri | Agri LMS |
|--|----------|----------|
| Count of External Facing Ips | 0 | 0 |
| Count of other Appliances (LB, DPG etc.) | 0 | 0 |

Details of third party:

| Name of the Third Party/ Vendor | Location | Services offered / Purpose of Integration | Supply Chain Control Point Report Available / To be Reviewed |
|---------------------------------|----------|---|--|
| | | | |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | |
|----------------------------|--------------|--|----------------------------------|
| National Portal/JanSamarth | Within India | To facilitate the flow of leads which are uploaded to National Portal to the LOS-AGRI application. | 43 point control point report. |
| CERSAI | Within India | For all Agri borrowings for limit above 5 lakhs, CERSAI registration through LOS-AGRI is required. | Self-Declaration by Third Party. |
| SBOSS | Within India | To facilitate the flow of leads from FOS application | 43 point control point report. |

We confirm that, all the Existing Software/Applications/APIs/URLs/Infra owned/managed by our department are included in the list and that all the details provided above are correct.

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



CSR 2024-25– Scope Collection Document
Department Name: IT-CORP & SME LOANS

APPLICATIONS IN SCOPE-

| S / N | Name of Application | Type of application (web/mobile /backend process) | Criticality | Exposed to (Internet/ Public NW) | No. of Devices for VA/SCD | | | | | Source Code | | App sec | | No. of web Services | No. Of Fire wall Rules | No. of API |
|-------|---------------------|---|-------------|----------------------------------|---------------------------|--------------|--------------|--------------|-------|-------------|--------------|------------------|----------------------------|---------------------|------------------------|------------|
| | | | | | OS | DB | App | Web | Total | LoC | Language | No of user roles | Input pages/ Dynamic pages | | | |
| 1 | LLMS | Web | Medium | Intranet | 12 PR 12 DR | 2 PR 2 DR | 6 PR 6 DR | 4 PR 4 DR | 24 | | Java | NA | NA | | | Approx 70 |
| 2 | OTS/SSC | Web | High | Internet | 4 PR 4 DR | 1 PR 1 DR | 1 PR 1 DR | 2 PR 2 DR | 8 | 1.4+ L | Java, Spring | NA | NA | - | 11 | |
| 3 | MBC | API | Medium | API | 4 PR 4 DR | 1 PR | 2 PR 2 DR | 1 PR 1 DR | 8 | | | NA | NA | | | |



| | | | | | | | | | | | | | | | | |
|---|-------------------------|--------------------------|--------|----------|----------------|--------------|----------------|--------------|----|--|--|----|----|--|--|--|
| | | | | | | 1 DR | | | | | | | | | | |
| 4 | PSM | Web | Low | Intranet | 3 PR 3 DR | 1 PR 1 DR | 1 PR 1 DR | 1 PR 1 DR | 6 | | | NA | NA | | | |
| 5 | e-Proposal | Android | Low | Internet | 1 PR 1 DR | - | - | 1PR 1DR | 2 | | | NA | NA | | | |
| 6 | Project Vivek | Web | Low | Intranet | 11 PR 11 DR | 1PR 1DR | 9 PR 9 DR | 1 PR 1 DR | 22 | | | NA | NA | | | |
| 7 | APT | Web | Low | Intranet | 15 PR 15 DR | 2 PR 2 DR | 12 PR 12 DR | 1 PR 1 DR | 30 | | | NA | NA | | | |
| 8 | RM APP (Pratham APP) | Web and Mobile App | Medium | Extranet | 14 PR 14 DR | 2 PR 2 DR | 8 PR 8 DR | 4 PR 4 DR | 28 | | | NA | NA | | | |
| 9 | CLP | API | Medium | API | 8 PR 8 DR | 1 PR 1 DR | 4 PR 4 DR | 3 PR 3 DR | 16 | | | NA | NA | | | |

Count of External Facing IP's: 6

Count of other Appliances (LB, DPG etc.):

- LLMS Lite (LB- 2 PR, 2 DR)
- LLMS (LB – 1 PR, 1 DR)



- RM APP (LB- 2 PR, 2 DR)
- CLP (LB- 2 PR, 2 DR)

Details of Third Party:

| Application Name | Third Party involved | Type of Integration | Via | Purpose |
|--------------------|----------------------|---------------------|--------------------|---------------------------------|
| LLMS | NeSL | API | EIS | DDE |
| LLMS | NSDL | API | EIS | PAN Validation |
| LLMS | NATIONAL PORTAL | API | EIS | Lead Sourcing |
| LLMS | CGTMSE | API | EIS | CG PAN Fetch |
| LLMS | ZED Portal | API | EIS | Zero Effect Zero Defect Ratings |
| LLMS | CIBIL | API | Bank's Proxy / MBC | Credit Reports |
| LLMS | Onlinepsbloans | API | CLP | Lead Sourcing |
| MBC | CIBIL | API | Bank's Proxy | Credit Reports |
| MBC | CRIF HIGHMARK | API | Bank's Proxy | Credit Reports |
| MBC | EXPERIAN | API | Bank's Proxy | Credit Reports |
| MBC | EQUIFAX | API | Bank's Proxy | Credit Reports |
| LLMS Lite | NESL | API | EIS | DDE |
| LLMS Lite | CRIF HIGHMARK | API | MBC | Credit Reports |
| Project Vivek | NSDL | API | EIS | PAN Validation |
| Advanced Pace Tool | NSDL | API | EIS | PAN Validation |



CSR 2024-2025 – Scope collection document

Department Name: Enterprise Integration Services

| S/ N | Name of Application | Submodule Name | No of Firewall rules | Criticality | Type of application (web/mobile /backend process | Exposed to (Internet/Public NW) | No. of Devices for VA/SCD | | | | | Source Code | | Appsec | | No. of web Services | No. of API |
|---------|----------------------------|---|----------------------|-------------|--|---------------------------------|---------------------------|----|-----|-----|-------|-------------|----------|------------------|---|---------------------|------------|
| | | | | | | | OS | DB | App | Web | Total | LoC | Language | No of user roles | Input pages/Dynamic pages | | |
| 1 | Miscellaneous applications | SGBS Admin, SI Reconciliation, PMScheme MIS, PMJJBY GST | | High | Front End Application | Intranet | | | | | | 40,000 | .NET | 1 | SGBS Admin- 15 SI Reconciliation - 1 PMScheme MIS - 8 PMJJBY GST - 3 | 6 | 6 |
| 2 | API Infrastructure | NA | | High | Web Services | Intranet and Public | | | | | | 27 Lac | IIB | NA | NA | NA | 1030 |

Engaging CAT-I Competent ISSPs from GITC empaneled vendors and ISD empaneled vendors for Comprehensive Security Review of Applications of IT-SF, IT-INB , IT-CMP & SCFU , IT-CINB & YB , IT- NETWORK, IT-PE-I , IT-CLOUD SOLUTION , IT – DATA CENTRE, IT-SP-II, IT-YONO , IT- CB DEV , IT-CB-TECH OPS, IT-NBC, IT-RETAIL LOAN , IT- AGRI TECH, IT-CORP & SME, IT-EIS , IT- TRADE FINANCE (FY 2024-25) Department



| | | | | | | | | | | | | | |
|---|---------|----|-----|-----|-----|----------|-----|----|----|---|-------------------------|----|----|
| 3 | API HUB | NA | 228 | Low | Web | Internet | 493 | NA | NA | 2 | Single Page Application | NA | NA |
|---|---------|----|-----|-----|-----|----------|-----|----|----|---|-------------------------|----|----|

Count of External Facing IPs: 4

Count of other Appliances (LB, DPG etc): 45



CSR 2024-2025– Scope Collection Document
Department Name: IT Trade Finance

| Sl No | Name of Application | Criticality | No. of Devices for VA/SCD | | | | | Source Code | | No of Firewall Rules | No. of web Services | No. of API |
|-------|---------------------|-------------|---------------------------|----|-----|-----|-------|-------------|--|----------------------|---------------------|------------|
| | | | OS | DB | App | Web | Total | LoC | Language | | | |
| 1 | EE | High | 26 | 5 | 6 | 4 | 41 | NA | Java | 33 | 6 | 0 |
| 2 | CSIG | High | 12 | 4 | 4 | 4 | 24 | NA | Java Spring | 13 | 1 | 0 |
| 3 | TRUST | Medium | 10 | 2 | 6 | 2 | 10 | 1,30,000 | Java Spring | 10 | 0 | 0 |
| 4 | TRRACS | Medium | 6 | 2 | 2 | 2 | 6 | 9,10,000 | Java (Back End) Frameworks : UI - JSF Hibernate & SPring | 7 | 0 | 1 |
| 5 | CTCP | Medium | 6 | 2 | 2 | 2 | 6 | 3,40,000 | Java(backend) Frame Works - Angular - (UI), Spring, Hibernate | 10 | 0 | 0 |

Third Party / Vendors where Sensitive data flows outside Bank

| Name: Integration with Third Party / Vendor | Location | Services Offered / Purpose | 28 Point Control Report Available / to be reviewed. |
|---|----------|----------------------------|---|
| ----- Nil ----- | | | |