



REQUEST FOR PROPOSAL
FOR

**Engagement of Managed Security Service Provider for Cyber
Security Defense center (CSDC) under CSCoE in bank
environment for a period of Three Years**

Ref: SBI/GITC/ISD/2025/2026/1434

Dated : 12.02.2026

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

Part-I

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

37	CODE OF INTEGRITY AND DEBARMENT/BANNING
38	TERMINATION FOR DEFAULT
39	FORCE MAJEURE
40	TERMINATION FOR INSOLVENCY
41	TERMINATION FOR CONVENIENCE
42	DISPUTES RESOLUTION
43	GOVERNING LANGUAGES
44	APPLICABLE LAW
45	TAXES AND DUTIES
46	TAX DEDUCTION AT SOURCES
47	TENDER FEE
48	EXEMPTION OF EMD AND TENDER FEE
49	NOTICES

Part-II

Appendix	Index
A	BID FORM
B	BIDDER'S ELIGIBILITY CRITERIA
C	TECHNICAL ELIGIBILITY CRITERIA
D	BIDDER DETAILS
E	SCOPE OF WORK AND PAYMENT SCHEDULE
F	INDICATIVE PRICE BID
G	BANK GUARANTEE FORMAT
H	PENALTIES
I	SERVICE LEVEL AGREEMENT
J	NON-DISCLOSURE AGREEMENT
K	PRE-BID QUERY FORMAT
L	FORMAT FOR SUBMISSION OF CLIENT REFERENCES
M	PRE-CONTRACT INTEGRITY PACT
N	FORMAT FOR EMD BANK GUARANTEE

Contents

1.	SCHEDULE OF EVENTS	5
2.	INVITATION TO BID:.....	8
3.	DISCLAIMER:	10
4.	DEFINITIONS:.....	11
5.	SCOPE OF WORK:	12
6.	ELIGIBILITY AND TECHNICAL CRITERIA:	12
7.	COST OF BID DOCUMENT:.....	13
8.	CLARIFICATION AND AMENDMENTS ON RFP/PRE-BID MEETING:	13
9.	CONTENTS OF BID DOCUMENT:.....	14
10.	EARNEST MONEY DEPOSIT (EMD):.....	14
11.	BID PREPARATION AND SUBMISSION:	16
12.	DEADLINE FOR SUBMISSION OF BIDS:	18
13.	MODIFICATION AND WITHDRAWAL OF BIDS:.....	18
14.	PERIOD OF BID VALIDITY AND VALIDITY OF PRICE QUOTED IN REVERSE AUCTION (RA):	19
15.	BID INTEGRITY:.....	19
16.	BIDDING PROCESS/OPENING OF TECHNICAL BIDS:	19
17.	TECHNICAL EVALUATION:	20
18.	EVALUATION OF INDICATIVE PRICE BIDS AND FINALIZATION:	21
19.	CONTACTING THE BANK:	22
20.	POWERS TO VARY OR OMIT WORK:	24
22.	WAIVER OF RIGHTS:.....	25
23.	CONTRACT AMENDMENT:.....	26
24.	BANK'S RIGHT TO ACCEPT ANY BID AND TO REJECT ANY OR ALL BIDS:	26
25.	BANK GUARANTEE:	26
27.	SERVICES & MODEL OF ENGAGEMENT	26
31.	PENALTIES:	31
32.	RIGHT TO VERIFICATION:.....	32
33.	RIGHT TO AUDIT:	32
34.	SUBCONTRACTING:	33
35.	VALIDITY OF AGREEMENT:	33
36.	LIMITATION OF LIABILITY:.....	33
37.	CONFIDENTIALITY:.....	34
39.	DELAY IN SERVICE PROVIDER'S PERFORMANCE:	34
40.	SERVICE PROVIDER'S OBLIGATIONS:	35
41.	TECHNICAL DOCUMENTATION: (DELETE, WHICHEVER IS NOT APPLICABLE)	36
42.	INTELLECTUAL PROPERTY RIGHTS AND OWNERSHIP:	38
43.	LIQUIDATED DAMAGES:.....	40
44.	CONFLICT OF INTEREST:.....	40
45.	CODE OF INTEGRITY AND DEBARMENT/BANNING:.....	41
46.	TERMINATION FOR DEFAULT:.....	45
47.	FORCE MAJEURE:.....	46
48.	TERMINATION FOR INSOLVENCY:	47
49.	TERMINATION FOR CONVENIENCE:	47
50.	DISPUTES RESOLUTION:	47
51.	GOVERNING LANGUAGE:	47
52.	APPLICABLE LAW:.....	48
53.	TAXES AND DUTIES:	48
54.	TAX DEDUCTION AT SOURCE:	49
55.	TENDER FEE:	50
56.	EXEMPTION OF EMD AND TENDER FEE:	50
57.	NOTICES:.....	51
	APPENDIX –A	53
	APPENDIX-B	57
	APPENDIX-C	64
	ANNEXURE C4	ERROR! BOOKMARK NOT DEFINED.

APPENDIX-D.....	67
APPENDIX-E	68
APPENDIX-F	84
APPENDIX-G	86
APPENDIX-H	88
APPENDIX-I.....	91
APPENDIX-J	ERROR! BOOKMARK NOT DEFINED.
APPENDIX-L	99
APPENDIX-M	100
APPENDIX-N	101
APPENDIX-O.....	109
APPENDIX-P	112

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)	Shri Varghese Anil, Deputy General Manager, Incident Response, ISD, dgmisd.ir@sbi.co.in ; Contact Person: John Peter Email: john.peter@sbi.co.in Mobile No.: 9789059436 Pre-bid queries mail copy to be marked to dgmisd.ir@sbi.co.in;john.peter@sbi.co.in Address State Bank Global IT Centre, Ground Floor, A Wing, Sector 11, CBD Belapur, Navi Mumbai-400614
2	Bid Document Availability including changes/amendments, if any to be issued	RFP may be downloaded from Bank's website https://sbi.bank.in/ procurement news from 12.02.2026
3	Last date for requesting clarification	Upto 23.55 on 19.02.2026 All communications regarding points / queries requiring clarifications shall be given in writing or by e-mail.
4	Pre - bid Meeting at (venue)	From 12.00 to 13.00 at 20.02.2026 through online meeting or physically
5	Clarifications to queries raised at pre-bid meeting will be provided by the Bank.	https://etender.sbi/SBI and Bank website on 24.02.2026

6	Last date and time for Bid submission	Upto 15.30 on 06.03.2026 (date)	
7	Address for submission of Bids (Please incorporate details of e-Procurement Agency portal wherein online bid has to be submitted)	https://etender.sbi/SBI	
8	Date and Time of opening of Technical Bids	06.03.2026 at 16.00 Authorized representatives of Bidders may be present online during opening of the Technical Bids. However, Technical Bids would be opened even in the absence of any or all of Bidders representatives.	
9	Opening of Indicative Price Bids	Indicative price bid of technically qualified bidders only will be opened on a subsequent date.	
10	Reverse Auction	On a subsequent date which will be communicated to such Bidders who qualify in the Technical Bid.	
11	Tender Fee	Rs. 20,000/- Amount should be deposited in A/c No: 4897932113433 IFSC: SBIN0011343 Account Name: Subsidy Inward Remittance Mode: NEFT and RTGS only Tender fee will be non-refundable.	
12	Earnest Money Deposit	Rs.30,00,000/- (Rupees Thirty Lakh only) Amount should be deposited in A/c No: 4897932113433 IFSC: SBIN0011343 Account Name: Subsidy Inward Remittance Mode: NEFT and RTGS only Or EMD should be in the form of a bank guarantee. EMD shall be valid upto 180 days from bid submission date. Bidder should deposit EMD and Tender Fee separately.	
13	Bank Guarantee	10 %of the Project Cost	Performance Security in form of BG should be valid for Three year(s)

Engagement of Managed Security Service Provider for
Cyber Security Defense center (CSDC) under CSCoE in
bank environment



			and three months from the effective date of the Contract.
14	Contact details of e-Procurement agency appointed for e- procurement	e-Procurement Technologies LTD – CMMI5 Nithya Vallavar E -procurement Technologies Limited. Address: A- 201/208, Wall Street – II, Opp. Orient Club, Ellisbridge, Ahmedabad – 380006, Gujarat,India Contact: Nithya@eptl.in Phone: 7859800609	

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).

- 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.

This Request for Proposal (RFP) has been issued by **the Bank** on behalf of **SBG** and the Bank sponsored Regional Rural Banks (RRBs) Engagement of Managed Security Service Provider for setting up Cyber Security Defense center (CSDC) under CSCoE in bank environment for a period of Three Years. Through the engagement of competent SME resources—L1 (6 resources), L2 (6 resources), and L3 (3 resource)—from an Information Security Service Provider, this initiative ensures comprehensive coverage across all levels of CSCoE project for a period of three year.

The proposed engagement shall be supported by competent resources possessing expertise across multiple cybersecurity domains, ensuring end-to-end coverage of detection, investigation, response, and assurance activities. The deployed resources

shall collectively cover the following skillsets, aligned to their respective responsibility levels:

A. Threat Intelligence Analysts and Deception Technology Analysts:

These resources shall support continuous monitoring, alert analysis, contextual enrichment, and validation of security events. Responsibilities include identifying potential threats, correlating intelligence inputs, validating alerts generated from deception and monitoring technologies, distinguishing false positives from true security incidents, and providing actionable intelligence inputs to incident response teams. Resources shall additionally support advanced correlation, trend analysis, and threat scenario development in collaboration with other security and IT teams.

- i. Should be able to perform threat hunting to uncover the security gaps or identify any persistent threats.
- ii. Proactively hunt for advanced threats, indicators of compromise (IOCs), and attacker techniques across networks, endpoints, cloud, and identity systems
- iii. Develop and execute threat-hunting hypotheses based on threat intelligence, MITRE ATT&CK, and emerging adversary tactics

B. Digital Forensics and Incident Response (DFIR) Specialists

DFIR resources shall be responsible for detailed incident investigation, forensic analysis, evidence collection, timeline reconstruction, and root cause analysis of confirmed security incidents. These resources shall support containment, remediation guidance, escalation handling, regulatory and audit support, and preparation of detailed investigation and RCA reports. DFIR SMEs shall provide strategic oversight, forensic methodology guidance, and assurance on investigation quality and compliance with regulatory and legal requirements.

C. Red Teaming, Ethical Hacking, Experts

Red Teaming and Ethical Hacking experts shall provide advisory support for proactive security posture enhancement, including identification of control gaps, attack simulation insights, and validation of detection and response effectiveness. These resources shall support improvement of security controls, incident detection logic, and response playbooks, and provide strategic recommendations to strengthen the Bank's overall cybersecurity resilience.

This multi-skill, multi-tiered resource model ensures operational effectiveness at the monitoring level, depth in investigation and response, and strategic oversight for

continuous improvement, governance, and regulatory compliance across the Bank's security ecosystem.

- The resources deployed or the bidder should assist bank in
 - i. Establishing industry-leading standards and best practices for adoption across the Bank, its subsidiaries, and the wider BFSI sector.
 - ii. Driving capability building via advanced training programs, certifications, and hands-on labs for Bank employees.
 - iii. Conducting cutting-edge threat research and sharing findings with regulators, industry bodies, and academia.

Analyze logs, telemetry, endpoint data, and network traffic to uncover stealthy or persistent threat

- 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 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.

Bank at its own discretion may extend the contract for another 2 years on same terms and conditions with nominal increment (not exceeding 8% per resource who have demonstrated excellent capabilities) as per Bank's prescribed policy, provided resource has worked for at least 6 months in SBI.

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:

“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.

- i. **“Bidder/Channel Partner”** means an eligible entity/firm submitting the Bid in response to this RFP.
- ii. **“Bid”** means the written reply or submission of response to this RFP.

- iii. **“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.
- iv. **“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.
- v. **“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.
- vi. **“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.
- vii. **Annual Maintenance Contract (AMC)** - It would be the annual cost of maintenance/upkeep/updation of product or specified hardware and software.

5. **SCOPE OF WORK:**

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

The Bank may, at its sole discretion, provide remote access to its information technology system to IT Service Provider through secured Virtual Private Network

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 and technical criteria as mentioned in this RFP document.
 - (a) If any Bidder submits Bid on behalf of Principal/OEM, the same Bidder shall not submit a Bid on behalf of another Principal/OEM under the RFP. Bid submitted with option of multiple OEMs shall also be considered bid submitted on behalf of multiple OEM.

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

(c) Subcontracting/hiring of external resources is not permitted.

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

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):

- i. The Bidder shall furnish EMD for the amount and validity period mentioned in Schedule of Events of this RFP.
- ii. EMD is required to protect the Bank against the risk of Bidder's conduct.

- iii. The EMD should be directly credited to the designated account as mentioned in Schedule of Events. Proof of remittance of EMD in the designated account should be enclosed with the technical bid.

If EMD is directly credited to designated account, proof of remittance of EMD in the designated account should be enclosed with the technical bid. However, if EMD is in form of Bank Guarantee, scanned copy of original EMD Bank Guarantee should be uploaded on portal of e-Procurement agency along with technical bid. Original EMD Bank Guarantee should be [delivered through registered post/courier](#) or given in person to the Bank at the address specified in Schedule of Event Sl. No. 1, within the bid submission date and time for the RFP.

- iv. Any Bid not accompanied by EMD for the specified amount and not submitted to the Bank as mentioned in this RFP will be rejected as non-responsive.
- v. The EMD of the unsuccessful Bidder(s) would be refunded/returned by the Bank within 2 weeks of the Bidder being notified as being unsuccessful.
- vi. The EMD of successful Bidder will be discharged upon the Bidder signing the Contract and furnishing the Bank Guarantee for the amount and validity as mentioned in this RFP, which should be strictly on the lines of format placed at **Appendix-H**.
- vii. No interest is payable on EMD.

viii. The EMD may be forfeited:-

- (b) if a Bidder withdraws his Bid during the period of Bid validity specified in this RFP; or
- (c) if a technically qualified Bidder do not participate in the auction by not logging in, in the reverse auction tool; or
- (d) if a Bidder makes any statement or encloses any form which turns out to be false / incorrect at any time prior to signing of Contract; or
- (e) if the successful Bidder fails to accept Purchase Order and/or sign the Contract with the Bank or furnish Bank Guarantee, within the specified time period in the RFP.
- ix. If EMD is forfeited for any reasons mentioned above, the concerned Bidder may be debarred from participating in the RFPs floated by the Bank/this department, in

future, as per sole discretion of the Bank.

11. BID PREPARATION AND SUBMISSION:

- i. The Bid is to be submitted separately for technical and Price on portal of e-Procurement agency for Engagement of Managed Security Service Provider for Cyber Security Defense center (CSDC) under CSCoE in bank environment for a period of Three Years **RFP No Ref: SBI/GITC/ISD/2025/2026/1434 dated 12.02.2026**. 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.
 - (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** Engagement of Managed Security Service Provider for Cyber Security Defense center (CSDC) under CSCoE in bank environment **of Three-Year RFP dated 12.02.2026** in response to the **SBI/GITC/ISD/2025-2026/1434 dated 12.02.2026** should contain only indicative Price Bid strictly on the lines of **Appendix-F. Indicative Price Bid for** Engagement of Managed Security Service Provider for Cyber Security Defense center (CSDC) under CSCoE in bank environment **for a period of Three Years RFP dated 12.02.2026** in response to the **RFP No: SBI/GITC/ISD/2025/2026/1434 dated 12.02.2026** 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.

iv. Documents mentioned below are to be uploaded on E-Tender Portal:

- a. Technical Bid covering letter/Bid form on the lines of Appendix-A on Bidder's letter head.
- b. Bidder's information as per Annexure A on bidder's letter head.
- c. Bank may ask for word copy of all the technical evaluation formats (Annexure C1 to C3) from all interested Vendors after opening of online technical bids.
- d. Audited balance sheets and profit and loss account statement for last 2 years
- e. A copy of board resolution or power of attorney showing that the signatory has been duly authorized to sign the tender document.
- f. Response to all points of the technical evaluation format should be as per Annexure C.
- g. Non-Disclosure Agreement as per Annexure D
- h. Compliance Statement as per Annexure E

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 a certificate as per **Appendix-G** from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content requirement for ‘Class-I local supplier’/ ‘Class-II local supplier’ as the case may be.

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

iv. Bank will notify successful Bidder in writing by way of issuance of purchase order through letter or fax/email that its Bid has been accepted. The selected Bidder has to return the duplicate copy of the same to the Bank within **7 working days**, duly Accepted, Stamped and Signed by Authorized Signatory in token of acceptance.

- v. The successful Bidder will have to submit Non-disclosure Agreement, Bank Guarantee for the amount and validity as desired in this RFP and strictly on the lines of format given in appendix of this RFP together with acceptance of all terms and conditions of RFP.
- vi. Copy of board resolution and power of attorney (POA wherever applicable) showing that the signatory has been duly authorized to sign the acceptance letter, contract and NDA should be submitted.
- vii. The successful Bidder shall be required to enter into a Contract with the Bank and submit the Bank Guarantee, within 30 days from issuance of Purchase Order or within such extended period as may be decided by the Bank.
- viii. Till execution of a formal contract, the RFP, along with the Bank's notification of award by way of issuance of purchase order and Service Provider's acceptance thereof, would be binding contractual obligation between the Bank and the successful Bidder.
- ix. The Bank reserves the right to stipulate, at the time of finalization of the Contract, any other document(s) to be enclosed as a part of the final Contract.
- x. Failure of the successful Bidder to comply with the requirements/terms and conditions of this RFP shall constitute sufficient grounds for the annulment of the award and forfeiture of the 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. SIGNING OF MASTER SERVICE LEVEL AGREEMENT (MSLA)

SBI will notify successful bidder(s) in writing by letter in duplicate or email/ fax that its bid has been accepted. The Selected bidder(s) must return the duplicate copy to the Bank within 7 working days duly Accepted, Stamped and Signed by Authorized Signatory in token of acceptance.

The successful bidder(s) shall be required to enter into a contract/Master SLA with the Bank, within 30 days of intimation of successful bidder or within such extended period as may be decided by the Bank along with the letter of acceptance, Non-Disclosure Agreement (NDA), BG and other terms and conditions as may be determined by the Bank to be necessary for the due performance of the work in accordance with the Bid and acceptance thereof.

Copy of board resolution or power of attorney showing that the signatory has been duly authorized to sign the acceptance letter, contract and NDA should be submitted.

The contract/agreement will be based on bidder's offer document with all its enclosures, modifications arising out of negotiation /clarifications etc., and will include project plan – phases & milestones and schedule, copies of all necessary documents, licenses, certifications etc.

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.

22. 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.

23. CONTRACT AMENDMENT:

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

24. 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.

25. 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.

26. SERVICES & MODEL OF ENGAGEMENT

The Bank proposes to engage an Information Security Service Provider to manage Cyber Security Defense Center (CSDC)-Managed services under CSCoE a dedicated, multi-disciplinary cybersecurity team to support threat intelligence operations, digital forensics and incident response, and red teaming / ethical hacking activities.

The engagement shall follow a tiered operating model (L1, L2, and L3) to ensure continuous monitoring, in-depth investigation, proactive security validation, and strategic oversight. The bidder shall be responsible for end-to-end execution of the scope of work, adherence to timelines, and delivery of all defined outcomes during the contract period. They will also be responsible for delivering reports duly signed by an authorized person to the bank's coordinating team. The bidder must ensure adherence to timelines, failing which the bank reserves the right to levy penalties as defined in the RFP.

A Project Manager / Team Lead, designated by the successful bidder, shall act as the single point of contact for the Bank and shall be accountable for overall coordination, resource management, reporting, and service quality. The Project Manager/Team Lead will report directly to the bank's coordination team, facilitating seamless collaboration and ensuring alignment with the bank's objectives. Regular updates, performance reviews, and consultations will be conducted to monitor progress and ensure the delivery of high-quality results aligned with the bank's security requirements.

27. DEPLOYMENT OF RESOURCES:

Resource Allocation and Availability

- All deployed resources shall meet the minimum educational, professional, and technical qualification criteria specified in this RFP.
- Resources shall possess relevant experience in one or more of the following domains:
 - i. Threat Intelligence/ threat hunting and Deception Technology Operations.
 - ii. Digital Forensics and Incident Response (DFIR).
 - iii. Red Teaming, Penetration Testing and Ethical Hacking.
- L1 resources shall have experience in monitoring, alert validation, data collection, solution configuration and SOP-driven operational activities.
- L2 resources shall have advanced expertise in investigation, correlation, forensic analysis, adversary techniques, and analytical reporting.
- L3 SMEs shall have extensive experience in cybersecurity strategy, governance, complex incident handling, and advisory roles within regulated environments.

- Resources should have prior exposure to working in SOC environments, cyber forensic investigation agencies, incident response teams, or security assessment engagements.
- Initially the bidder to deploy 15 resources as per RFP and later if required additional resources to be onboarded if required by Bank on the same rate contract discovered during the Reverse Auction.
- Proposed resources shall be subject to vetting and approval by the Bank.
- Count of resources shall be interchanged based among the different skillsets based on the requirement from bank

Onboarding and Training

- All deployed resources shall undergo formal onboarding covering the Bank's security architecture, policies, SOPs, escalation matrix, and compliance requirements.
- The bidder shall ensure continuous training and skill enhancement to keep resources updated on emerging threats, tools, attack techniques, and regulatory requirements.
- Knowledge transfer, documentation, and handover processes shall be mandatory during onboarding and any transition.

Reporting Structure

- The Project Manager / Team Lead designated by the Service Provider shall report directly to the Bank's designated coordination team.
- Responsibilities of the Project Manager / Team Lead shall include:
 - Task allocation and workload management.
 - Monitoring performance and service quality.
 - Ensuring timely submission of reports and deliverables.
 - Facilitating coordination with internal stakeholders and committees.
 - Periodic review meetings, performance assessments, and consultations shall be conducted as prescribed by the Bank.

Timeliness and Penalties

- 60% Resources shall be deployed and made operational within 20 working days from the date of acceptance of the Purchase Order (PO).
- Remaining 40% deployment in 90 days
- The PO shall be accepted by the bidder within 7 working days of issuance.
- Any delay in deployment, replacement, or delivery of services may attract penalties as defined in the RFP.

- The bidder must ensure uninterrupted resource availability. Any delays in deployment or non-availability of resources without prior notice may attract penalties as outlined in the RFP.

Replacement and Backup Resources

- The bidder shall ensure that any resource exiting the engagement is replaced with an equally or better qualified resource within 30 working days
- Identified backup resources shall be trained in advance to ensure continuity of operations.
- Replacement resources shall be subject to the same vetting and approval process as original resources.
- If the resources are found suitable, and does not have eligible professional certificate, the bidder to make sure the candidate complete the eligible professional certificate within 6 months from date of joining.

Location and Work Hours

- Resources must operate from a location approved by the bank(i.e. In Navi Mumbai or anywhere in India if needed).
- Resources will adhere to standard working hours, with provisions for extended support during critical incidents.

Documentation and Reporting

- All resources shall maintain accurate and complete documentation of activities, findings, investigations, and recommendations as per Bank-defined formats.
- Documentation shall support audit, compliance, regulatory, and management review requirements.
- Reports shall be submitted on a daily, weekly, monthly, or ad-hoc basis as specified/required by the Bank.

Deliverables For the Engagement

Operational Deliverables

- Continuous monitoring and analysis outputs (alerts, indicators, events)
- Validation of security events and escalation records
- Detailed investigation and analysis reports for confirmed incidents
- Findings from forensic analysis, threat hunting, or red team activities
- Identification of recurring patterns, weaknesses, and risk areas

- Manage threat intelligence solutions, platform.

Governance and Policy Deliverables

- Recommendations for strengthening security controls, processes, and frameworks
- Inputs for refinement of incident handling, investigation, and escalation procedures
- Documentation of governance mechanisms and operational improvements

Reports and Documentation

- Periodic operational and performance reports
- Comprehensive investigation and assessment reports
- Executive summaries for critical or high-impact incidents
- Evidence supporting compliance with internal policies and regulatory requirements

Stakeholder Engagement Deliverables

- Periodic presentations and briefings to Bank-designated committees or senior management
- Coordination artefacts for internal teams and external stakeholders during incidents or assessments
- Training and knowledge-sharing documentation for operational teams

Strategic Deliverables

- Periodic security posture assessments and maturity evaluations
- Strategic analysis of emerging threats and adversary trends
- Long-term recommendations to enhance the Bank's cybersecurity resilience and preparedness

*******All the Bidders have to share the resource profile along with contact details for evaluation of the quality/Job Knowledge of the resources.**

28. CANCELLATION OF CONTRACT

The Bank shall have the right to cancel/terminate the contract with the selected bidder at any time during the contract period, by giving a written notice of at least 1 (One) month, for any valid reason, including but not limited to the following:

- i. Laxity in following security standards laid down by the Bank
- ii. Excessive delay in execution of orders/tasks/requirements placed by the Bank
- iii. Discrepancies / deviations in the agreed processes and/or products
- iv. Violation of Terms & Conditions stipulated in this RFP.

v. Failure in deployment of resources as mentioned in the RFP

If the performance of the bidder is not satisfactory in an assignment awarded to them, the Bank may terminate the assignment and impose penalty for the same. The penalty may extend up to the contract amount.

In the event of SBI terminating the Contract in whole or in part, SBI may assign, upon such terms and in such manner, as it deems appropriate, bidder shall be liable to the Bank for excess costs for such similar services and services those are undelivered.

Bank reserves the right to report any misconduct on part of the selected bidder during empanelment or non-reporting of any material observation having impact on SBI reputation or threat to Information owned and held with SBI or its Subsidiaries / Joint Ventures or non-following the clauses of this RFP and future agreement/SLA to be signed with SBI to RBI, SEBI, Cert-in, NCIIPC etc. or notify it publicly.

Bank also reserves it's right to blacklist the defaulting bidder on a temporary or permanent basis.

29. RESPONSIBILITIES OF THE BIDDERS:

The bidders, while providing services to the Bank, are expected to provide qualitative and substantive deliverables as per the scope of work defined in this RFP.

30. PENALTIES:

The Bank will be authorized to forfeit the amount of Bank Guarantee if the bidder fails to comply with the contracted terms and conditions.

SLA and Penalty for Resource Deployment

Sr. No.	Service Level Category	SLA Measurement & Failure Indicator	Penalty Calculation
1	Onsite Resource Deployment	Deployment of less than 70% of the required resources	₹5,000 per unfulfilled resource per week
		Deployment of less than 50% of the required resources	₹7,000 per unfulfilled resource per week
		Deployment of less than 25% of the required resources	₹10,000 per unfulfilled resource per week

Note: Amounts will be rounded off.

Details can be found in as mentioned in **Appendix-H** of this RFP.

Bank will impose a maximum penalty of 20% of the overall service charges per quarter.

The maximum penalty due to non-adherence of SLA will not exceed 20% of the total cost of the project calculated up to and as on the date when such penalty is required to be charged. However, in addition to the above penalty, the Bank may invoke Bank Guarantee submitted by the bidder if the bidder fails to adhere to SLA or any of the terms & conditions in the RFP.

31. 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.

32. 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.

33. SUBCONTRACTING:

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

34. VALIDITY OF AGREEMENT:

The Agreement/ SLA will be valid for the period of 3 year(s) extendable upto further 2 years based on Bank's discretion. The Bank reserves the right to terminate the Agreement as per the terms of RFP/ Agreement.

35. 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.

36. CONFIDENTIALITY:

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

37. PERFORMANCE BANK GUARANTEE: 10% of the Contract Value drawn on a bank other than SBI, Validity of the Performance Bank Guarantee: Duration of the contract + 3 months.

38. 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).

39. 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. The Service Provider agrees to comply with the obligations arising out of the Digital Personal Data Protection Act, 2023, as and when made effective. Any processing of Personal Data by the Service Providers in the performance of this Agreement shall be in compliance with the above Act thereafter. The Service Provider shall also procure that any sub-contractor (if allowed) engaged by it shall act in compliance with the above Act, to the extent applicable. The Service Provider understands and

agrees that this agreement may have to be modified in a time bound manner to ensure that the provisions contained herein are in compliance with the above Act.

- ix. Service Provider agrees to comply with the guidelines contained in the Bank's IT Outsourcing Policy / IT Procurement Policy or any other relevant policy (ies) of the Bank, including any amendment thereto, along with compliance to all the Laws of Land and Statutory/Regulatory rules and regulations in force or as and when enacted during the validity period of the contract.

40. TECHNICAL DOCUMENTATION

For the scope of work described, the following technical documentation will be provided by the team but not limited to below

1. Incident Management Documentation (CSCOE Governance Role)

The CSCOE shall define and govern the standardized incident documentation framework to ensure consistency, traceability, and audit readiness across all security incidents.

CSCOE Responsibilities

1. Incident Management Documentation

- Incident Validation Reports: Logs of validated incidents, detailing false positives, true positives, and resolution steps.
- Preliminary Investigation Reports: Initial analysis performed on incidents by L1, including incident metadata and a summary of actions taken.
- Incident Escalation Logs: Detailed documentation of cases escalated from L1 to L2 and from L2 to L3, including reasons for escalation and initial findings.
- Root Cause Analysis (RCA) Reports: Detailed investigations for high-risk incidents, outlining root causes, impacts, and mitigation steps.
- Daily/Weekly/Monthly Incident Reports: Aggregated reports on incidents, metrics, trends, and patterns.
- Daily, weekly, and monthly consolidated incident dashboards
- Single source of truth for incident records
- Audit-ready incident trail with clear accountability
- Improved consistency across SOC, DFIR, and investigation teams

2. Policy Management and Governance Documentation (CSCOE Ownership)

Act as the custodian and governance authority for cybersecurity policies, standards, and

procedures.

- Maintain the master repository of cybersecurity policies and procedures
- Drive policy updates based on incident learnings, risk assessments, and regulatory changes
- Ensure alignment between policy intent and operational execution.
- Governance frameworks defining roles, responsibilities, and escalation paths
- Detection and control refinement records with approvals and testing outcomes
- Living policy framework aligned to real-world threats
- Strong governance and defensibility during audits and inspections

3. Technical Analysis, Forensics Investigations, RCA and Advisory Documentation

- Threat Analysis Reports: In-depth analysis of patterns and trends in incidents, threats to identify recurring threats or vulnerabilities.
- System Improvement Recommendations: Recommendations for improving Threat Intelligence, Deception technology tools, detection rules, or related systems, Advisory notes recommending systemic and architectural improvements
- Best Practices Guidelines: Documented guidance on security best practices tailored for the bank's ecosystem.
- Training Materials: Manuals, guides, or presentations for L1 and L2 teams on the effective use of tools and adherence to policies.

4. Strategic and Executive-Level Documentation (CSCOE)

The CSCOE shall be responsible for converting operational and technical findings into executive-level intelligence and strategic guidance.

- Prepare strategic cybersecurity posture reports for senior management
- Translate incident trends into business and risk impact narratives
- Provide inputs for Board-level and regulator-facing discussions
- Executive dashboards and strategic risk reports
- Program effectiveness and maturity assessments
- Regulatory compliance and supervisory reporting documentation
- Long-term cybersecurity roadmap and improvement recommendations
- Informed executive decision-making
- Clear visibility into cyber risk posture
- Alignment of cybersecurity initiatives with business objectives

5. Collaboration and Coordination Documentation (CSCOE Orchestration Role)

The CSCOE shall act as the central coordination hub across internal and external stakeholders during cybersecurity events and initiatives.

- Stakeholder Communication Logs: Records of interactions and decisions made with IT, security teams, senior management and external stakeholder such as industry experts, other industry peers not limited to BFSI.
- Meeting Minutes: Summaries of key discussions during meetings various stakeholders.
- Vulnerability Mitigation Plans: Plans created in collaboration with IT teams to address identified vulnerabilities.
- Govern cross-functional coordination during incidents and risk mitigation efforts
- Ensure accountability and follow-through on agreed actions
- Stakeholder communication and decision logs
- Meeting minutes with IT, Security, Compliance, Legal, and Business teams
- Joint remediation and mitigation plans with ownership and timelines
- Clear accountability and traceability
- Reduced coordination gaps during incidents
- Improved response efficiency and stakeholder alignment

6. Tools Performance and System Usage Documentation (CSCOE Assurance Role)

The CSCOE shall oversee **tool effectiveness, optimisation, and value realisation** across the cybersecurity technology stack.

- Define metrics to assess tool performance and coverage
- Review configuration changes and tuning outcomes
- Ensure optimal utilisation of security investments
- System configuration baselines and change records
- Tool performance and effectiveness assessments
- Knowledge base, lessons learned, and troubleshooting repositories for the bank
- Evidence-based assessment of tool effectiveness
- Continuous optimisation of security controls
- Preservation of organisational knowledge and continuity

41. 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 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.
- vi. 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.
- vii. 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.

42. LIQUIDATED DAMAGES:

If Service Provider fails to deliver and perform any or all the Services within the stipulated time, schedule as specified in this RFP/Agreement, the Bank may, without prejudice to its other remedies under the RFP/Agreement, and unless otherwise extension of time is agreed upon without the application of liquidated damages, deduct from the Project Cost, as liquidated damages a sum equivalent to 0.5% of total Project Cost for delay of each week or part thereof maximum up to 20% of total Project Cost. Once the maximum deduction is reached, the Bank may consider termination of the Agreement.

43. 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.

44. 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 empanelled list**

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

- Without prejudice to the rights of the Bank under Clause 39 " *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 EOI/RFP issued by the Bank during a period of 2 (two) years from the date of debarment.
 - Vendor fails to abide by the terms and conditions or to maintain the required technical/operational staff/equipment or there is change in its production/service line affecting its performance adversely, or fails to cooperate or qualify in the review for empanelment;
 - If Vendor ceases to exist or ceases to operate in the category of requirements for which it is empaneled;
 - Bankruptcy or insolvency on the part of the vendor as declared by a court of law; or
 - Banning by Ministry/Department or any other Government agency;
 - Other than in situations of force majeure, technically qualified Bidder withdraws from the procurement process or after being declared as successful bidder: (i) withdraws from the process; (ii) fails to enter into a Contract; or (iii) fails to provide performance guarantee or any other document or security required in terms of the RFP documents;
 - If the Central Bureau of Investigation/CVC/C&AG or Vigilance Department of the Bank or any other investigating agency recommends such a course in respect of a case under investigation;
 - Employs a Government servant or the Bank's Officer within two years of his retirement, who has had business dealings with him in an official capacity before retirement; or
 - Any other ground, based on which the Bank considers, that continuation of Contract is not in public interest.
 - If there is strong justification for believing that the partners/directors/proprietor/agents of the firm/company 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.

45. 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.

46. FORCE MAJEURE:

- i. Notwithstanding the provisions of terms and conditions contained in this RFP, neither party shall be liable for any delay in in performing its obligations herein if and to the extent that such delay is the result of an event of Force Majeure.
- ii. For the purposes of this clause, 'Force Majeure' means and includes wars, insurrections, revolution, civil disturbance, riots, terrorist acts, public strikes, hartal, bundh, fires, floods, epidemic, quarantine restrictions, freight embargoes, declared general strikes in relevant industries, Vis Major, acts of Government in their sovereign capacity, impeding reasonable performance of Service Provider and / or Sub-Contractor but does not include any foreseeable events, commercial considerations or those involving fault or negligence on the part of the party claiming Force Majeure.
- iii. If a Force Majeure situation arises, Service Provider shall promptly notify the Bank in writing of such condition and the cause thereof. Unless otherwise directed by the Bank in writing, Service Provider shall continue to perform its obligations under the Contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.
- iv. If the Force Majeure situation continues beyond 30 (thirty) days, either party shall have the right to terminate the Agreement by giving a notice to the other party. Neither party shall have any penal liability to the other in respect of the termination of the Agreement as a result of an event of Force Majeure. However, Service Provider shall be entitled to receive payments for all services actually rendered up to the date

of the termination of the Agreement.

47. 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.

48. 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.

49. DISPUTES RESOLUTION:

- 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 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.
- ii. 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.

50. GOVERNING LANGUAGE:

The governing language shall be English.

51. 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.

52. 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.

53. 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.

54. TENDER FEE:

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

55. 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.

56. NOTICES:

Any notice given by one party to the other pursuant to this contract shall be sent to the other party in writing or by Fax and confirmed in writing to other Party's address. For all notices, the following shall be the current address:

The Group CISO,
Information Security Department,
Ground Floor, A Wing
State Bank Global IT Centre
Sector 11, CBD Belapur
Navi Mumbai – 400 614
Email: gciso@sbi.co.in

The notice shall be effective when delivered or on the notice's effective date whichever is later. Any change in the address will be communicated to the Service Provider, and all future notices shall be sent to the updated address.

Part-II

BID FORM (TECHNICAL BID)

[On Company's letter head]

(To be included in Technical Bid)

Date: _____

To:

Deputy General Manager (Incident Response)
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. Ref: SBI/GITC/ISD/2025/2026/1434 dated 12.02.2026

**Engagement of Managed Security Service Provider for setting up Cyber Security
Defense center (CSDC) under CSCoE in bank environment for a period of Three Years**

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, favor, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Bank, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.
- iv. We undertake that we will not resort to canvassing with any official of the Bank, connected directly or indirectly with the bidding process to derive any undue advantage. We also understand that any violation in this regard, will result in disqualification of bidder from further bidding process.
- v. It is further certified that the contents of our Bid are factually correct. We have not sought any deviation to the terms and conditions of the RFP. We also accept that in the event of any information / data / particulars proving to be incorrect, the Bank will have right to disqualify us from the RFP without prejudice to any other rights available to the Bank.
- vi. We certify that while submitting our Bid document, we have not made any changes in the contents of the RFP document, read with its amendments/clarifications provided by the Bank.
- vii. We agree to abide by all the RFP terms and conditions, contents of Service Level Agreement as per template available at **Appendix-J** of this RFP and the rates quoted therein for the orders awarded by the Bank up to the period prescribed in the RFP, which shall remain binding upon us.
- viii. On acceptance of our technical bid, we undertake to participate in Reverse auction by way of login in Reverse auction tool. In case of declaration as successful Bidder on completion of Reverse auction process, we undertake to complete the formalities as specified in this RFP.
- ix. The commercial bidding process will be through the reverse auction process to be conducted by the Bank or a company authorized by the Bank. We understand that our authorized representative who would participate in the reverse auction process would be possessing a valid digital certificate for the purpose.

- x. Till execution of a formal contract, the RFP, along with the Bank's notification of award by way of issuance of purchase order and our acceptance thereof, would be binding contractual obligation on the Bank and us.
- xi. We understand that you are not bound to accept the lowest or any Bid you may receive and you may reject all or any Bid without assigning any reason or giving any explanation whatsoever.
- xii. We hereby certify that our name does not appear in any "Caution" list of RBI / IBA or any other regulatory body for outsourcing activity.
- xiii. We hereby certify that on the date of submission of Bid for this RFP, we do not have any past/ present litigation which adversely affect our participation in this RFP or we are not under any debarment/blacklist period for breach of contract/fraud/corrupt practices by any Scheduled Commercial Bank/ Public Sector Undertaking/ State or Central Government or their agencies/departments.
- xiv. We hereby certify that 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)

Engagement of Managed Security Service Provider for
Cyber Security Defense center (CSDC) under CSCoE in
bank environment



Duly authorised to sign Bid for and on behalf of

_____ **Seal of the company.**

Appendix-B

Bidder's Eligibility Criteria

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

S. No.	Eligibility Criteria	Compliance (Yes/No)	Documents to be submitted
1.	The Bidder must be an Indian Company/ LLP /Partnership firm registered under applicable Act in India.		Certificate of Incorporation issued by Registrar of Companies and full address of the registered office along with Memorandum & Articles of Association/ Partnership Deed.
2.	The Bidder (including its OEM, if any) must comply with the requirements contained in O.M. No. 6/18/2019-PPD, dated 23.07.2020 order (Public Procurement No. 1), order (Public Procurement No. 2) dated 23.07.2020 and order (Public Procurement No. 3) dated 24.07.2020		Bidder should specifically certify in Appendix A in this regard and provide copy of registration certificate issued by competent authority wherever applicable.
3.	The Bidder individually and not Group Company should have average minimum turnover of Rs. 29.00 Crores during last three financial years (2022-23 and 2023-24 and 2024-25)		Copy of the audited financial statement for required financial years. (Certificate from statutory auditor for preceding/current year may be submitted.) Annexure B2
4.	The Bidder should be profitable organization on the basis of profit before tax (PBT) for at least 02 (two) out of last 03 (three) financial years mentioned in para 3 above.		Copy of the audited financial statement along with profit and loss statement for corresponding years and / or Certificate of the statutory auditor.

5.	Bidder should have experience of minimum 5 (five) years in providing Cyber Security managed Services/Cyber Security Resources as mentioned in scope of work for BFSI sector Appendix E		Copy of the order and / or Certificate of completion of the work. The Bidder should also furnish user acceptance report.
6.	The Bidder (including its OEM, if any) should either be Class-I or Class-II local supplier as defined under this RFP.		Certificate of local content to be submitted as per Appendix-G .
7.	Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects as required under this RFP . (Start and End Date of the Project to be mentioned) in the past (At least 4 client references are required, put which 2 should be from BFSI sector) Experience Supporting Documents-Purchase order/Work Order/Client Reference to be furnished		Bidder should specifically confirm on their letter head in this regard as per Appendix-M
8.	The Bidder must have at least one hundred fifty (150) full time technically qualified consulting personnel with at least twenty five (25) possessing requisite cyber security domain expertise as on RFP publication date with at least five (05) years of relevant experience. Any of the international accreditation like ISC2/ISACA/EC-Council/Comptia/SANS/Offsec/PM / eCTHP / GCTI / CTIA / GREM I/ CRTP / CRTE which has minimum 45 hrs of education curriculum ,employed with them since the last 2 years deployed in Information security /Cybersecurity domain. The		Certificate from the HR representative or by the authorized signatory of the Bidder with the list of twenty-five (25) personnel with relevant experience and qualification along with their respective location.

	profile of the resources shared should be stationed in India.		
9.	Past/present litigations, disputes, if any (Adverse litigations could result in disqualification, at the sole discretion of the Bank)		Brief details of litigations, disputes related to product/services being procured under this RFP or infringement of any third party Intellectual Property Rights by prospective Bidder/ OEM or disputes among Bidder's board of directors, liquidation, bankruptcy, insolvency cases or cases for debarment/blacklisting for breach of contract/fraud/corrupt practices by any Scheduled Commercial Bank/ Public Sector Undertaking / State or Central Government or their agencies/ departments or any such similar cases, if any are to be given on Company's letter head.
10.	Bidders should not be under debarment/blacklist period for breach of contract/fraud/corrupt practices by any Scheduled Commercial Bank/ Public Sector Undertaking / State or Central Government or their agencies/ departments on the date of submission of bid for this RFP.		Bidder should specifically certify in Appendix A in this regard.
11	The Bidder should not have any Service Level Agreement pending to be signed with the Bank for more than 6 months from the date of issue of purchase order.		Bidder should specifically certify in Appendix A in this regard.
12	Engagement of the organization in the similar activities for last 5 years. Bidder should have experience of minimum 05 years in providing the Consultancy Services for establishing Cyber Security Centre of Excellence or any similar facility. Similar facility like Centre of		The bidders should provide Certificate of completion of the work/PO/contract details / statement of work/ SLA. Copy of the order and Certificate of completion of the work or Selfcertificate of project certified by the Authorized Signatory clearly

	Excellence in Cyber Crime & Fraud Prevention Centre, Security Operation Centre and Resilience Operation Centre.		demonstrating the status and the value of the project.
13	Existing IT partner/bidder in the Information Security Department providing similar kind of services in last 2 year from the date of RFP should have fulfilled 90% resource requirement as per the RFP. For existing ongoing RFP/Projects in ISD, bidder should have deployed 75% of resource fulfillment within 6 Months from date of PO.		A formal declaration or letter from their project manager confirming compliance with the 90% resource fulfillment rate over the specified period.
14	The bidder, if participating as Channel Partner of any OEM, then OEM should have a support center and level 3 escalation (highest) located in India. For OEMs, directly participating, the conditions mentioned above for support center remain applicable.		Bidder should specifically certify in Appendix A in this regard
15	Bidder should have experience of at least two (02) consulting projects involving managing Cyber Security Centre of Excellence or similar facility in Central / State Government / Banking & Financial Institution where at least one should be – a) BFSI and b) One engagement with an organization with on-roll Employee base > 10K or having balance sheet size of Rs 15,000/- crores		Completion certificates from the client; OR Self-certificate of project certified by the Authorized Signatory clearly demonstrating the status and the value of the project.

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

Eligibility criteria mentioned at SI No 3 to 5 in table above are relaxed for Startups subject to their meeting of quality and technical specifications. Bidder to note the followings:

- i. Start-up” company should enclose the valid Certificate of Recognition issued by Department for Promotion of Industry and Internal Trade (DPIIT), (erstwhile Department of Industrial Policy and Promotion), Ministry of Commerce & Industry, Govt. of India with the technical bid.
- ii. Bidder who solely on its own, fulfils each eligibility criteria condition as per the RFP terms and conditions and who are having Start-up company status, can claim exemption for eligibility criteria mentioned at SI No 3 to 5 in table above.
- iii. If all these conditions are not fulfilled or supporting documents are not submitted with the technical Bid, then all those Bids will be summarily rejected, and no queries will be entertained.

Name & Signature of authorized signatory

Seal of Company

****The above-mentioned criteria are mandatory in nature. The bidders should qualify all the above-mentioned eligibility criteria for being eligible to submit the bid which will later be evaluated as per the technical evaluation criteria mentioned in the RFP.**

Annexure B1

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			

Signature

Seal of Company

Please Note:

- Certificate of Incorporation and KYC of the Organization

Turnover of organization

For the period April 2021 to March 2024

<u>Sl No.</u>	<u>Turnover Details (Last 3 years)</u>	<u>Amt in Crores</u>
1	FY 2021-22	
2	FY 2022-23	
3	FY 2023-24	

Please Note:

- Audited balance sheet of the Organization

Signature

Seal of Company

Appendix-C

Technical – Evaluation Parameter

Sl. No	Criteria Description	Evidence Required	Yes/ No
1	At least 5 BFSI clients with proven experience in Information Security-Threat Intelligence/deception technology/Red teaming/Ethical Hacking (2 must be from BFSI) in the last 5 years.	Client Reference & Project Experience Table Annexure C1	
2	The Bidder should have a pool of full-time minimum at least 150 professionals who have experience in Threat Intelligence/deception technology/Red teaming/Ethical Hacking activity within India with at least one Security Certified Professional from offensive-security/ Licensed Penetration Tester (LPT) from EC-Council / ISC2/ ISACA /SANS/ Offsec /PMI as full-time employee. Kindly refer table A in Appendix E.	Annexure C2	
3	Resources – Relevant experience in Information Security, Threat Intelligence/deception technology/Red teaming/Ethical Hacking. L1/L2 resources must hold at least one certification Kindly refer table A in Appendix E.	Certification Copies (Valid and Active Status)	
4	Vendor resources must have strong written and verbal communication skills for incident reporting, stakeholder engagement, and training.	Sample Reports/Presentations/Training Material	
5	Required experience of manpower (key resources) as per Appendix E		
6	Compliance to SOW and Appendix E		
7	Compliance to all terms and conditions of the RFP and all Corrigendum issued		

Annexure C1

Assignments handled by the organization

(Assignments handled of minimum 5 distinct clients under Information / Cyber security domain (In BFSI sector) during the last five years(FY-2020-2025).) Among these 5 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 2020-21, 2021-22 ,2022-23, 2023-24 and 2024-25</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. in BFSI sector **having balance sheet of Rupees 10,000.00 Cr and above.**

Supporting Documents-Purchase order/Work Order/Client Reference to be furnished

Signature

Seal of Company

Skilled Information security resources currently available (Full time)

SI No.	Name of resource	Academic Qualification of the resource	Professional Qualification of the resource

Details of 25 resources to be provided.

Name & Signature of authorized signatory

Seal of Company

Appendix-D

Bidder Details

Details of the Bidder

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

Name & Signature of authorised signatory

Seal of Company

Scope of Work and Payment Schedule

**Engagement of Managed Security Service Provider for setting up Cyber Security
Defense center (CSDC) under CSCoE in bank environment for a period of Three Years**

Salient features:

The successful bidder shall manage the activities associated with **Cyber Security Centre of Excellence (CSCOE)** to provide centralized governance, technical assurance, strategic oversight, and continuous improvement of the Bank's cybersecurity operations based on the scope of the RFP

The CSCOE shall function as the **authoritative body** for standardization, quality assurance, risk visibility, and maturity enhancement across all cybersecurity activities.

Proactive Threat Identification through Threat Intelligence & Deception

This integrated model ensures end-to-end visibility, control, and continuous improvement across the cybersecurity lifecycle. The CSCOE shall leverage **Threat Intelligence and Deception Technology Analysts** to enable early identification of cyber threats, adversary techniques, and emerging attack patterns.

Key features include:

- Centralized threat intelligence correlation from internal and external sources
- Analysis of attacker behavior through deception assets (honeypots, decoys, fake credentials)
- Reduction of false positives through contextual validation
- Intelligence-driven prioritization of security risks

Structured Incident Investigation and Forensic Assurance (DFIR)

The CSCOE shall ensure **deep investigative capability** through **DFIR specialists**, providing technical rigor and defensibility for all major security incidents.

Key features include:

- Standardized forensic methodologies and investigation workflows
- Accurate incident timeline reconstruction and impact assessment
- Root Cause Analysis (RCA) and control gap identification
- Support for legal, audit, and regulatory requirements

Proactive Security Assurance through Red Teaming & Ethical Hacking

The CSCoE shall incorporate **Red Teaming and Ethical Hacking Experts** to proactively assess and strengthen the Bank's cyber defenses.

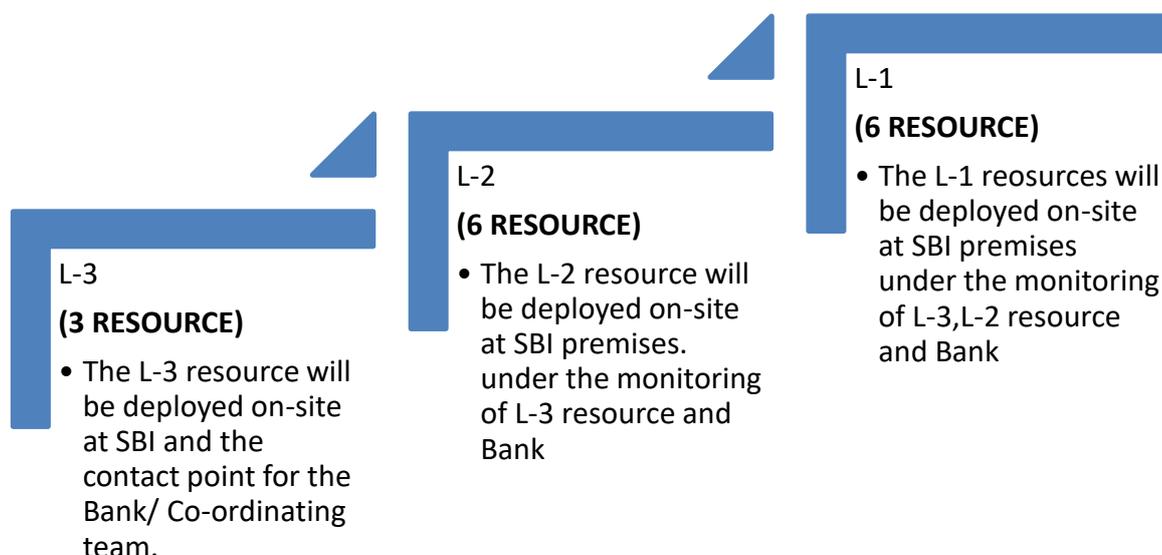
Key features include:

- Simulation of real-world attack scenarios and adversary techniques
- Identification of attack paths and systemic control weaknesses
- Validation of detection and response effectiveness
- Advisory recommendations to improve preventive and detective controls

MODEL OF ENGAGEMENT

The bidders should deploy 15 resources for review activities as per Skill-set and educational/ professional criteria of this RFP.

The Project manager/Team Lead has to be defined by the successful bidder who will be the contact point for the Bank and the job will be assigned to the respective contact person. The Successful bidder will be responsible for the complete execution of the jobs assigned and timely delivery of the duly signed reports by the authorized person.



The Project manager/ Team Lead will be assigned the job along with the defined timelines for the delivery of the job. The Successful bidder has to assure the timely delivery failing the same the Bank is authorized to levy penalty as defined in the RFP.

The Project manager/Team Lead has to report to the Co-ordinating team defined by the Bank.

- i. Total period of engagement – Three Year (from the date of Purchase order) which may be extended for additional 2 years with nominal increment of 8% per resource rate from existing contract value.
- ii. **Period of engagement & Leaves** – The period of engagement will be for continuous period (Three year). However, if there is a break from resource side, the bidder must provide for suitable alternate resource and proper knowledge transfer to be ensured between the two (outgoing & incoming) resources before allowing the existing resource to leave the site. Utilization of resources will be on man days basis.
- iii. **The Educational, professional qualifications and number years of experience: -**

Categorisation of Resource	Number of resources	Educational Qualification	Professional Qualification	Years of Experience
L-1	6	B.Sc (IT/CS)/B.E./ B.Tech/MCA /M.E./M.Tech	<p>Essential: Certified Ethical Hacker (EC-Council) / Computer Hacking Forensic Investigator (EC-Council) / CRTP / CRTE/ CTIA/ or equivalent certification agreed by bank which has minimum 45 hrs of education curriculum.</p> <p>Preferred: Certified SOC Analyst (EC-Council) / CompTIA Security+ / Cisco Certified CyberOps Associate</p> <p>Note: Resource deployed to have add on</p>	2-5 years

			certificate apart from CEH.	
L-2	6	B.Sc (IT/CS)/B.E./ B.Tech/MCA /M.E./M.Tech	<p>Essential: Certified Ethical Hacker (EC-Council) / Computer Hacking Forensic Investigator (EC-Council) / CRTP / CRTE/ CTIA/ or equivalent certification agreed by bank which has minimum 45 hrs of education curriculum.</p> <p>Preferred: Certified SOC Analyst (EC-Council) / CompTIA Security+ / Cisco Certified CyberOps Associate</p> <p>Note: Resource deployed to have addon certificate apart from CEH.</p>	5-8 years
L-3	3	B.Sc (IT/CS)/B.E./ B.Tech/MCA /M.E./M.Tech	<p>Essential: CISSP / OSCP / OSCE / eCTHP / GCTI / CTIA / GREM/ or equivalent certification agreed by bank which has minimum 45 hrs of education curriculum.</p> <p>Preferred: GCIA / GCIH / GCFA / GSEC / CCSP / Certified SOC Analyst (EC-Council)</p> <p>Any one of /Comptia/SANS/Offsec/ or equivalent</p>	8+ years

			<p>certification agreed by bank which has minimum 45 hrs of education curriculum</p> <p>Note: Resource deployed to have addon certificate apart from CISSP/CISM relevant to the role which are listed above.</p>	
--	--	--	--	--

Table A

There will be a mix of L1-6(Six) resource L2-6(Six) resources and L3-1(Three) resources proposed for the project.

The L3 resources would monitor the manpower, delivery and provide their expertise in reviewing the deliverables and signing off on the completeness of the activity from quality perspective. The L-3 resource would be the direct contact point for the Bank and the whole project management is to be handled by the same along with any specialized inputs required by the top management.

Detailed requirement of the specialization specific resources L-1 resources (**6 resource**) & **L-2 resources (6 resources) & L3 resource(3 resources)**:

Activities performed by resources /Specialization of the resource	Number of resources (L1)	Number of resources (L2)	Number of resources (L3)
Threat Intelligence Analysts/Deception Technology Analysts/ Threat Hunting Experts	2	2	1
Digital Forensics & Incident Response (DFIR)	2	2	1
Red Teaming & Ethical Hacking &	2	2	1
Sub total	6	6	3
Total			15

A total 6 L1, 6 L2 and 3 L3 resources to be deployed for a period of three years under this RFP , and the working days in a months shall be reckoned as 24 days for the purpose of calculating man-days and processing of bill. The billing will be done based on the below calculation, which will be billed once in quarterly.

A	B	C	C	D
Resources	number of day in month	Total Man-day in MONTH	Total Man-day in year B*12)	Total Man-day in three years month (C*3)
6	24	144	1728	5184
6	24	144	1728	5184
3	24	72	864	2592
			4320	12960

iv. Below is the scope of work, but not limited to

○ **Threat Intelligence & Deception Analysts:**

- Threat Intelligence and honeypot solution end to end Management in coordination with OEM.
- L1 (monitoring, enrichment), L2 (advanced correlation, trend analysis), L3 (strategic intelligence oversight).
- Continuous monitoring of internal security alerts, threat feeds, and intelligence sources relevant to the BFSI ecosystem.
- Collection, validation, and enrichment of Indicators of Compromise (IOCs), TTPs, and threat artefacts.
- Correlation of intelligence with internal events to determine relevance and potential business impact.
- Identification of emerging threats, attack campaigns, and adversary behavior patterns.
- Preparation of tactical and strategic threat intelligence reports, dashboards, and advisories.
- Input to risk assessments, preventive control tuning, and security awareness initiatives.
- Integration of threat intelligence into SOAR use cases and automated response workflows
- Periodic validation and tuning of honeypot/ deception coverage against current adversary TTPs
- Proactively hunt for advanced threats, indicators of compromise (IOCs), and attacker techniques across networks, endpoints, cloud, and identity systems

- Develop and execute threat-hunting hypotheses based on threat intelligence, MITRE ATT&CK, and emerging adversary tactics
 - Analyze logs, telemetry, endpoint data, and network traffic to uncover stealthy or persistent threats
 - Conduct deep-dive investigations into suspicious activity and confirm or dismiss potential threats
 - Collaborate with SOC, Incident Response, and Detection Engineering teams to escalate and remediate confirmed threats
 - Create, tune, and improve detection rules, alerts, and analytics based on hunting outcomes
 - Document findings, attack patterns, and lessons learned in clear technical reports
 - Track and research threat actors, malware campaigns, and zero-day techniques.
 - Should be able to perform threat hunting to uncover the security gaps or identify any persistent threats.
 - Proactively hunt for advanced threats, indicators of compromise (IOCs), and attacker techniques across networks, endpoints, cloud, and identity systems
 - Develop and execute threat-hunting hypotheses based on threat intelligence, MITRE ATT&CK, and emerging adversary tactics
- **DFIR Specialists:**
- Forensic activity and tool management.
 - L1 (initial evidence support), L2 (lead investigations, RCA), L3 (forensic oversight, complex cases).
 - Lead and support investigations of confirmed security incidents across endpoints, servers, networks, applications, email, and cloud environments.
 - Perform log analysis, memory analysis, network traffic analysis, and system forensics as applicable.

- Coordinate containment, eradication, and recovery actions with IT and security teams.
 - Collection, preservation, and analysis of digital evidence in a forensically sound and legally defensible manner.
 - Maintenance of chain-of-custody documentation and investigation artefacts.
 - Detailed reconstruction of incident timelines.
 - Identification of root causes, control gaps, and contributing factors.
 - Assessment of technical, operational, regulatory, and reputational impact.
 - Preparation of detailed investigation reports, RCA documents, and executive summaries.
 - Support internal audits, regulatory inspections, and supervisory queries.
 - Provide expert inputs during crisis situations and senior-management briefings.
 - Malware triage and behavioral analysis to support attribution and containment decisions
 - Post-incident lessons learned workshops and validation of corrective actions
- **Red Teaming & Ethical Hacking Experts:**
- L3 (primary advisory & assurance role) with L2 technical support as required.
 - Conduct controlled adversary simulation and ethical hacking exercises (with prior approval).
 - Simulate real-world attack scenarios to test preventive, detective, and response controls.
 - Identify exploitable weaknesses, misconfigurations, and attack paths.
 - Assess effectiveness of monitoring, detection logic, and response playbooks.
 - Provide advisory inputs to strengthen security architecture, detection capabilities, and response processes.

- Support post-incident reviews by mapping attacker techniques to defensive gaps.
- Risk-based prioritization of red team findings aligned to business criticality.
- Recommend improvements based on industry best practices and red team findings.
- Reporting to the Application Owner by logging a ticket in the incident management portal and assist them in understanding and mitigating vulnerabilities. Track all observation and incident tickets until they are closed.
- Conduct red team exercises simulating APT, ransomware, insider threat, and cybercrime campaigns. Participate/assist in Blue team exercise
- Emulate adversary TTPs aligned to MITRE ATT&CK
- Execute multi-stage attack chains including initial access, persistence, privilege escalation, lateral movement, command-and-control, and data exfiltration
- Develop custom attack payloads, scripts, and tools
- Exploit weaknesses in: Active Directory & Identity (Kerberos, NTLM, Active Directory Certificate Services) Endpoint security controls (EDR/EPP bypass) Network security (firewalls, segmentation, SMB, RDP)
- Bypass EDR, AV, SIEM, UEBA, MFA, DLP, and logging controls
- Develop and test living-off-the-land (LOLbins) techniques
- Map findings to MITRE ATT&CK, Cyber Kill Chain, and business risk
- Experience in working with following tools and platforms: Cobalt Strike, Metasploit Mimikatz, Rubeus, SecretsDump BloodHound, SharpHound, PowerView, CrackMapExec Burp Suite, Nmap, Nessus, Impacket GoPhish.

Web Application Penetration testing:

- Understanding of IT Security technology & processes particularly related to Web Applications and Network Security.

- Advanced Knowledge in vulnerability assessment, Penetration Testing & Ethical hacking across IT platforms used for hosting/implementing web application solutions.
- Should have experience in discovery, analysis, remediation, and monitoring cybersecurity vulnerabilities with respect to the organization's attack surface (Deep Web/ Dark Web Analysis).
- Ability to perform and review security assessment of web application to identify OWASP Top 10 related vulnerabilities.
- Ability to perform and review of vulnerability & Penetration testing, vulnerability closure, coordination, follow up & escalation with the asset owners.
- Ability to identify threats and vulnerabilities, map the identified vulnerabilities to corresponding attack categories, organizational processes, and policies.
- Understanding of real-world attack techniques & appropriate mitigations.
- Expertise in Web application Security vulnerabilities (SQL Injection, XSS, CSRF, IDOR etc) and various ways in which it can be exploited. Experience in secure code reviews to help the developers to remediate / triage vulnerabilities.
- Penetration Testing experience using tools like Burp suite/OWASP ZAP Proxy, Kali Linux, Qualys/Nessus, Nmap, HCL AppScan etc.
- Knowledge of at least one programming knowledge such as C, C++, Python, Java, ASP.NET will be preferred.
- Threat modeling for applications during design and major change phases.
- Validation of API security (REST/GraphQL) including auth, rate limiting, and data exposure.
- Review of third-party libraries, SDKs, and supply-chain risks.
- Support DevSecOps by integrating security testing into CI/CD pipelines.

Mobile Application Penetration Testing:

- Advanced Knowledge in vulnerability assessment, Penetration testing & Ethical hacking across IT platforms used for hosting/implementing mobile application solutions.
 - Ability to perform and review security assessment of mobile (Android/iOS) application to identify OWASP TOP 10 vulnerabilities.
 - Ability to identify threats and vulnerabilities, map the identified vulnerabilities to corresponding attack categories, organizational processes, and policies.
 - Ability to perform and review regular Vulnerability Assessment, Penetration Testing & Ethical Hacking on Mobile Applications (Android/IOS), vulnerability closure, coordination & follow up with the Asset owners.
 - Expertise in security testing of mobile applications (Static/Dynamic/Memory Analysis) and experience on Dynamic instrumentation tools like JADX, ADB, MoBSF, Burp suite, Frida/Objection, Magisk etc.
 - Knowledge of Reverse Engineering on APK & applications and reverse engineering tools.
 - Hands-on experience on Root Detection and SSL pinning bypass techniques.
 - Knowledge on Android Development.
 - Basic Knowledge of at least one programming knowledge such as C, C++, Python, Java, ASP.NET will be preferred.
- **Common activities**
- Ownership and governance of cybersecurity policies, standards, and SOPs.
 - Continuous refinement of policies based on threat intelligence, DFIR findings, and red team outcomes.
 - Definition of incident handling frameworks, escalation matrices, and approval workflows.
 - Assurance of investigation quality, documentation completeness, and compliance readiness.
 - Standardized incident, investigation, and escalation documentation.

- Periodic operational, tactical, and strategic reports.
- Executive dashboards and Board-level summaries.
- Maintenance of a central knowledge repository capturing lessons learned, playbooks, and best practices.

Other Requirements

- Working hours as per Bank ISD working hours or as per project requirement.
 - Work location in Navi Mumbai Locations.
 - Basic Strong understanding of information security principles.
 - Capability to manage high-pressure situations and complex escalations.
 - Strong leadership and collaboration skills for coordinating with multiple stakeholders.
 - Visionary mindset with the ability to identify emerging threats and industry trends.
 - Strong decision-making abilities under critical circumstances.
 - Exceptional stakeholder management and collaboration skills
 - Any other technical work assigned to be fulfilled by the resources of the bidder.
- v. The selected bidder must submit the Profile, KYC, Background Check report, Police verification, educational qualification and experience of the resources going to be deputed for the assignment to the department. The Information Security Department (ISD) discretion is final in accepting the resources for the project. ISD will also decide on the count of resources that would be taken from the bidder.
- vi. Each individual resource(s) deployed for the purpose must sign the non-disclosure agreement as per the IS Policy of the Bank, wherever required.
- vii. The Onboarded resources will be deployed to similar project or work on any ISD project in bank with 2- 5 days notice.
- viii. The resources has to be deployed on-site at SBI ,GITC ,Navi Mumbai, Belapur office or any other centre in Mumbai/Navi Mumbai.
- ix. Resources need to work on all working Saturday if Bank has working day. (Minimum 24 days in a month)
- x. In Case of emergency resource may have to work on Sundays and holidays also.
- xi. The biometric attendance tracker for the resources will be done and the resources must work for minimum 8 hrs a day excluding breaks.

- xii. Invoice on quarterly basis can be raised along with the proper submission of the status reports. It has to be ensured by the bidder that the respective resources has to be engaged during the full tenure of bill claimed. The Bill will only be paid for the actual services provided.
- xiii. The bidders desirous of submitting their quotes must accept all the terms and conditions as above. No exceptions are accepted in the bid. In case of bids submitted with any exceptions, the bid will be rejected.
- xiv. A formal communication protocol will be established between Bidder and SBI as per the following schedule for the activity status update:

Weekly Status update Report: To provide an update on the activities performed and any interim observations.

Monthly status update report: To provide a monthly update on activities performed.

As needed/ via email or in person: To communicate roadblocks and potential high-risk items

- xv. Weightage for the payment of the bill in terms of resources engaged will be as under:

SI No	Category of resource	Percentage of rate in comparison with L-1
1	L-2	1.42% of L-1
2	L-3	1.73% of L-1

- xvi. Payment of the resources will be made once in 3 months.
- xvii. Any Other job as defined by ISD from time to time

DEPLOYMENT OF RESOURCES:

The bidders should deploy 6-8(Minimum 3-L1, 3-L2,1-L3) resources within 20 days and remaining resources within next 90 days as per Skill-set and educational/professional criteria of this RFP within from the date of declaration of the successful bidder in the reverse auction. The detailed profile of the resources is to be provided. 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 30 working days from the date of intimation. In case of resource resignation/termination during the deployed period, the successful bidder has to make necessary arrangements 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.

**The bidder should also be in a position to deploy additional 25% of the total resource strength as and when required by the Bank within 30 days. The cost of the additional resource will be on the same lines as per the finalized cost of the successful bidder.

Qualifications and Skillsets

- Each resource must meet the educational, professional, and technical skill requirements specified in the RFP, including certifications relevant to requirement of the RFP.

Onboarding and Training

- All resources must undergo onboarding sessions to familiarize themselves with the bank's tools, policies, and escalation procedures.
- The successful bidder will be responsible for providing ongoing training to ensure the team's proficiency in evolving threats and technologies.

Reporting Structure

- a. The Project Manager/Team Lead appointed by the bidder will act as the central point of contact for coordinating with the bank's team.
- b. The Project Manager will allocate tasks, monitor performance, and ensure that deliverables are submitted within the defined timelines.

Timeliness and Penalties

- Resources must be deployed and operational within 20 days of the contract award.
- The bidder must ensure uninterrupted resource availability. Any delays in deployment or non-availability of resources without prior notice may attract penalties as outlined in the RFP.

Replacement and Backup Resources

- The bidder must ensure that any resource leaving the project is replaced with an equally qualified individual within 30-45 working days.
- Backup resources should be identified and trained in advance to maintain continuity in operations.

Location and Work Hours

- Resources must operate from a location approved by the bank, with the flexibility to work onsite or remotely as required.
- Resources will adhere to standard working hours, with provisions for extended support during critical incidents.

Documentation and Reporting

- The bidder will ensure that all team members maintain proper documentation of activities, incident analyses, and deliverables as per the bank's guidelines.
- Daily, weekly, and monthly progress reports must be submitted to the bank's Steering Committee or designated point of contact.

Deliverable for the Engagement:

Operational Deliverables

- Detailed documentation of alerts, distinguishing between false positives and true positives.
- Logs and findings from initial analysis conducted by L1 resources.
- Documentation of incidents escalated to L2 and L3 teams, including the reasons and priority levels.
- Detailed reports on high-risk incidents investigated by the L2 and L3 teams.
- Insights into recurring patterns and vulnerabilities identified during incident investigations.
- Steps taken to address specific vulnerabilities or incident causes.

Governance and Policy Deliverables

- Suggested updates and refinements to existing policies based on incident trends and analysis.
- Documentation of improvements made to detection rules, Threat analysis and thresholds.
- Detailed documentation of the frameworks developed for incident handling and escalation.

Reports and Documentation

- Summarized status of alerts, Threat Intelligence reports, validations, and escalations.
- Comprehensive reports on incidents, resolutions, and team performance.
- Executive-level summaries for critical or high-risk incidents.
- Evidence of compliance with data protection regulations and internal policies.

Stakeholder Engagement Deliverables

- Periodic reports and presentations to the bank's team.
- Documentation used for onboarding and upskilling L1 and L2 resources.
- Plans for engaging with internal teams, senior management, and external parties during incidents.

Strategic Deliverables

- Strategic analysis of risks posed by specific incidents or trends.
- Defined KPIs covering detection effectiveness, investigation quality, response timeliness, and governance outcomes.
- Periodic maturity assessments and improvement roadmap
- Executive dashboards and Board-level summaries
- Maintenance of a central knowledge repository capturing lessons learned, playbooks, and best practices

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.

Any relaxation in experience or qualification criteria shall require approval from a competent authority not below the level of DGM / SVP.

*******All the Bidders has to share the resource profile along with contact details for evaluation of the quality/Job Knowledge of the resources.**

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.

Name of the Bidder:

Sr. No.	Type of services / Items	Quantity/No of Resources	Rate per item/Per resource per day rate (as applicable)	Total amount in Rs.	Proportion to Total Cost (in percentage) #
1.	L1 Resources	6		Rate per item/Per resource per day rate* 6	58.23%
2.	L2 Resources	6	Rate of L1 * 1.42	Rate of L1 * 1.42*6	39.27%
3.	L3 Resource	03	Rate of L1 * 1.73	Rate of L1 * 1.73*3	2.5%
	Total Cost *				

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

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

Breakup of Taxes and Duties

As applicable

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

Name & Signature of authorised signatory

Seal of Company

Appendix-G

Certificate of Local Content

Date:

To,

Dear Sir,

Ref.: SBI/GITC/ISD/2025/2026/1434 dated 12.02.2026

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

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:

Sl 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:

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. Ref: SBI/GITC/ISD/2025/2026/1434 dated 12.02.2026
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 notwithstanding 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

Other terms and Penalties

- i. If existing Service Provider is breach of this obligation, they shall be liable for paying a penalty to an extent of 100% 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. The overall CAP of Penalties is 20% of PO Value.

Table A

Sr. No.	Service Level Category	SLA Measurement & Failure Indicator	Penalty Calculation
1	Onsite Resource Deployment	Deployment of less than 70% of the required resources	₹5,000 per unfulfilled resource per week
		Deployment of less than 50% of the required resources	₹7,000 per unfulfilled resource per week
		Deployment of less than 25% of the required resources	₹10,000 per unfulfilled resource per week

Table B

S.No	Description	Liquidated Damages/LD*
1	Service Provider shall provide acknowledgement within 2 Working Days from receipt of PO.	0.05% of PO Value for delay of per day in providing acknowledgement subject to maximum up to 0.20% of PO Value.
2	Service Provider shall provide PO acceptance within 5 Working Days from date of acknowledgement of PO.	0.25% of PO Value for delay of per day in providing acceptance subject to maximum up to 1.5% of PO Value
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 10 Working Days from the date of acceptance of PO or within 10 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	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.
5	Unauthorized absence of onsite resources from Bank's premises.	0.25% of PO Value for each instance subject to maximum up to 1.5% of PO Value
6	Delay in providing the opinions / Delay in submitting reports/ Minutes of Meeting(s)/ any other deliverables as mentioned under Scope of work or the date advised by the Bank	0.25% of PO Value for delay of per week in providing any or all CVs subject to maximum up to 1.5% of PO Value
7	Non-adherence to the timelines of the various phases of the project	2% of PO Value for delay of per week in non-adherence to timeline subject to maximum up to 15.00% of PO Value
8	The resources to be onboarded within 7-15 days from the date of finalization of the resources by the Bank or a later period that may be specified in the PO.	2% of PO Value for delay of per week in onboarding of any or all resources subject to maximum up to 15.00% of PO Value

- SLA: Stamp paper- 2% of the project cost+Rs.500 or as per latest government norms
- NDA document stamp paper-Rs.500 or as per latest government norms.
- The aggregate of yearly SLA penalties will be limited to 20% of the Project Cost

Note: Suitable Penalties metric may be devised keeping in view of the criticality of the proposed procurement. An example of Indicative format has been provided in Software and Service Level Agreement for guidance.

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		

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

Format for Submission of Client References

To whosoever it may concern

Particulars	Details
Client Information	
Client Name	
Client address	
Name of the contact person and designation	
Phone number of the contact person	
E-mail address of the contact person	
Project Details	
Name of the Project	
Start Date	
End Date	
Current Status (In Progress / Completed)	
Size of Project	
Value of Work Order (In Lakh) (only single work order)	

Name & Signature of authorised signatory

Seal of Company

Appendix-N

PRE CONTRACT INTEGRITY PACT
(TO BE STAMPED AS AN AGREEMENT)

General

This pre-Bid pre-contract Agreement (hereinafter called the Integrity Pact) is made on _____ day of the month of _____ 201 , between, on the one hand, the State Bank of India a body corporate incorporated under the State Bank of India Act, 1955 having its Corporate Centre at State Bank Bhavan, Nariman Point, Mumbai through its _____ Department / Office at Global IT Center at CBD Belapur, _____ 400614, (hereinafter called the "BUYER", which expression shall mean and include, unless the context otherwise requires, its successors) of the First Part

And

M/s _____ represented by Shri _____, Chief Executive Officer/ Authorised signatory (hereinafter called the "BIDDER/Seller which expression shall mean and include, unless the context otherwise requires, its / his successors and permitted assigns of the Second Part.

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

WHEREAS the BIDDER is a private company/public company/Government undertaking/partnership/registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is an Office / Department of State Bank of India performing its functions on behalf of State Bank of India.

NOW, THEREFORE,

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

- Enabling the BUYER to obtain the desired service / product at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement; and

- Enabling BIDDERS to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the BUYER will commit to prevent corruption, in any form, by its officials by following transparent procedures.

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

1. Commitments of the BUYER

- 1.1 The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organisation or third party related to the contract in exchange for an advantage in the bidding process, Bid evaluation, contracting or implementation process related to the contract.
- 1.2 The BUYER will, during the pre-contract stage, treat all BIDDERS alike, and will provide to all BIDDERS the same information and will not provide any such information to any particular BIDDER which could afford an advantage to that particular BIDDER in comparison to other BIDDERS.
- 1.3 All the officials of the BUYER will report to the appropriate authority any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.
- 1.4 In case any such preceding misconduct on the part of such official(s) is reported by the BIDDER to the BUYER with full and verifiable facts and the same is prima facie found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the BUYER and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings under the contract would not be stalled.

2. Commitments of BIDDERS

- 2.1 The BIDDER commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its Bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following:
- 2.2 The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER, connected directly or indirectly with the bidding process, or to any person, organisation or third party related to the contract in exchange for any

advantage in the bidding, evaluation, contracting and implementation of the contract.

- 2.3 The BIDDER further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with State Bank of India for showing or forbearing to show favour or disfavour to any person in relation to the contract or any other contract with State Bank of India.
- 2.4 Wherever applicable, the BIDDER shall disclose the name and address of agents and representatives permitted by the Bid documents and Indian BIDDERS shall disclose their foreign principals or associates, if any.
- 2.5 The BIDDER confirms and declares that they have not made any payments to any agents/brokers or any other intermediary, in connection with this Bid/contract.
- 2.6 The BIDDER further confirms and declares to the BUYER that the BIDDER is the original vendors or service providers in respect of product / service covered in the Bid documents and the BIDDER has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER, nor has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.
- 2.7 The BIDDER, at the earliest available opportunity, i.e. either while presenting the Bid or during pre-contract negotiations and in any case before opening the financial Bid and before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the BUYER or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.
- 2.8 The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, Bid evaluation, contracting and implementation of the contract.
- 2.9 The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.
- 2.10 The BIDDER shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the BUYER as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.
- 2.11 The BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.
- 2.12 The BIDDER shall not instigate or cause to instigate any third person to commit

any of the actions mentioned above.

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

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

3. **Previous Transgression**

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

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

4. **Earnest Money (Security Deposit)**

4.1 While submitting commercial Bid, the BIDDER shall deposit an amount (specified in RFP) as Earnest Money/Security Deposit, with the BUYER through any of the mode mentioned in the RFP / Bid document and no such mode is specified, by a Bank Draft or a Pay Order in favour of State Bank of India from any Bank including SBI . However payment of any such amount by way of Bank Guarantee, if so permitted as per Bid documents / RFP should be from any Scheduled Commercial Bank other than SBI and promising payment of the guaranteed sum to the BUYER on demand within three working days without any demur whatsoever and without seeking any reasons whatsoever. The demand for payment by the BUYER shall be treated as conclusive proof for making such payment to the BUYER.

4.2 Unless otherwise stipulated in the Bid document / RFP, the Earnest Money/Security Deposit shall be valid upto a period of five years or the complete conclusion of the contractual obligations to the complete satisfaction of both the BIDDER and the BUYER, including warranty period, whichever is later.

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

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

5. Sanctions for Violations

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

- (i) To immediately call off the pre contract negotiations without assigning any reason and without giving any compensation to the BIDDER. However, the proceedings with the other BIDDER(s) would continue, unless the BUYER desires to drop the entire process.
- (ii) The Earnest Money Deposit (in pre-contract stage) and/or Security Deposit/Performance Bond (after the contract is signed) shall stand forfeited either fully or partially, as decided by the BUYER and the BUYER shall not be required to assign any reason therefore.
- (iii) To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER.
- (iv) To recover all sums already paid by the BUYER, and in case of an Indian BIDDER with interest thereon at 2% higher than the prevailing Base Rate of State Bank of India, while in case of a BIDDER from a country other than India with interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the BIDDER from the BUYER in connection with any other contract for any other stores, such outstanding could also be utilized to recover the aforesaid sum and interest.
- (v) To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the BIDDER, in order to recover the payments, already made by the BUYER, along with interest.
- (vi) To cancel all or any other Contracts with the BIDDER. The BIDDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER.
- (vii) To debar the BIDDER from participating in future bidding processes of the BUYER or any of its Subsidiaries for a minimum period of five years, which may be further extended at the discretion of the BUYER.
- (viii) To recover all sums paid, in violation of this Pact, by BIDDER(s) to any middleman or agent or broker with a view to securing the contract.
- (ix) Forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.
- (x) Intimate to the CVC, IBA, RBI, as the BUYER deemed fit the details of such events for appropriate action by such authorities.

- 5.2 The BUYER will be entitled to take all or any of the actions mentioned at para 5.1(i) to (x) of this Pact also on the Commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defined in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.
- 5.3 The decision of the BUYER to the effect that a breach of the provisions of this Pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the Independent Monitor(s) appointed for the purposes of this Pact.

6. Fall Clause

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

7. Independent Monitors

- 7.1 The BUYER has appointed Independent Monitors (hereinafter referred to as Monitors) for this Pact in consultation with the Central Vigilance Commission (Names and Addresses of the Monitors to be given).

नाम	Shri Satyajit Mohanty	Smt. Rashmi Verma
संवर्ग	IPS (Retd.)	IAS (Retd.)
संपर्क नंबर	Mobile No.9437110622	Mobile No. 9810735544
ई-मेल आइडी	satyajitmohanty88@gmail.com	rashmi.naveenverma@gmail.com

- 7.2 The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.
- 7.3 The Monitors shall not be subjected to instructions by the representatives of the parties and perform their functions neutrally and independently.
- 7.4 Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings. Parties signing

this Pact shall not approach the Courts while representing the matters to Independent External Monitors and he/she will await their decision in the matter.

- 7.5 As soon as the Monitor notices, or has reason to believe, a violation of this Pact, he will so inform the Authority designated by the BUYER.
- 7.6 The BIDDER(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the BIDDER. The BIDDER will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractor(s) with confidentiality.
- 7.7 The BUYER will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the parties. The parties will offer to the Monitor the option to participate in such meetings.
- 7.8 The Monitor will submit a written report to the designated Authority of BUYER/Secretary in the Department/ within 8 to 10 weeks from the date of reference or intimation to him by the BUYER / BIDDER and, should the occasion arise, submit proposals for correcting problematic situations.

8. Facilitation of Investigation

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

9. Law and Place of Jurisdiction

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

10. Other Legal Actions

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

11. Validity

- 11.1 The validity of this Integrity Pact shall be from date of its signing and extend upto 5 years or the complete execution of the contract to the satisfaction of both the BUYER and the BIDDER/Seller, including warranty period, whichever is later. In

case BIDDER is unsuccessful, this Integrity Pact shall expire after six months from the date of the signing of the contract, with the successful Bidder by the BUYER.

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

12. The parties hereby sign this Integrity Pact at _____ on _____

For BUYER

Name of the Officer.

Designation

Office / Department / Branch

State Bank of India.

For BIDDER

Chief Executive Officer/

Authorised Signatory

Designation

Witness

1

2

Witness

1.

2.

Note: This agreement will require stamp duty as applicable in the State where it is executed or stamp duty payable as per Maharashtra Stamp Act, whichever is higher.

Appendix-O

FORMAT FOR EMD BANK GUARANTEE

To:

EMD BANK GUARANTEE FOR

NAME OF SERVICES TO STATE BANK OF INDIA TO MEET SUCH REQUIRMENT
AND PROVIDE SUCH SERVICES AS ARE SET OUT IN THE
SBI/GITC/ISD/2025/2026/1434 dated 12.02.2026

WHEREAS State Bank of India (SBI), having its Corporate Office at Nariman Point,
Mumbai, and Regional offices at other State capital cities in India has invited Request to
provide _____(name of Service) as are set out in the Request for Proposal SBI:
Ref SBI/GITC/ISD/2025/2026/1434 dated 12.02.2026

2. It is one of the terms of said Request for Proposal that the Bidder shall furnish a Bank
Guarantee for a sum of Rs. _____/-(Rupees _____ only) as Earnest
Money Deposit.

3. M/s. _____, (hereinafter called as Bidder, who are our constituents
intends to submit their Bid for the said work and have requested us to furnish guarantee in
respect of the said sum of Rs. _____/-(Rupees _____ only)

4. NOW THIS GUARANTEE WITNESSETH THAT

We _____ (Bank) do hereby agree with and undertake to the
State Bank of India, their Successors, assigns that in the event of the SBI coming to the
conclusion that the Bidder has not performed their obligations under the said conditions of
the RFP or have committed a breach thereof, which conclusion shall be binding on us as well
as the said Bidder, we shall on demand by the SBI, pay without demur to the SBI, a sum of
Rs. _____/-(Rupees _____ Only) that may be demanded by SBI.
Our guarantee shall be treated as equivalent to the Earnest Money Deposit for the due
performance of the obligations of the Bidder under the said conditions, provided, however,
that our liability against such sum shall not exceed the sum of Rs. _____/-(Rupees
_____ Only).

5. We also agree to undertake to and confirm that the sum not exceeding Rs. _____/-(
Rupees _____ Only) as aforesaid shall be paid by us without any demur
or protest, merely on demand from the SBI on receipt of a notice in writing stating the
amount is due to them and we shall not ask for any further proof or evidence and the notice
from the SBI shall be conclusive and binding on us and shall not be questioned by us in any

respect or manner whatsoever. We undertake to pay the amount claimed by the SBI, without protest or demur or without reference to Bidder and notwithstanding any contestation or existence of any dispute whatsoever between Bidder and SBI, pay SBI forthwith from the date of receipt of the notice as aforesaid. We confirm that our obligation to the SBI under this guarantee shall be independent of the agreement or agreements or other understandings between the SBI and the Bidder. This guarantee shall not be revoked by us without prior consent in writing of the SBI.

6. We hereby further agree that –

- a) Any forbearance or commission on the part of the SBI in enforcing the conditions of the said agreement or in compliance with any of the terms and conditions stipulated in the said Bid and/or hereunder or granting of any time or showing of any indulgence by the SBI to the Bidder or any other matter in connection therewith shall not discharge us in any way our obligation under this guarantee. This guarantee shall be discharged only by the performance of the Bidder of their obligations and in the event of their failure to do so, by payment by us of the sum not exceeding Rs. _____/- (Rupees _____ Only)
- b) Our liability under these presents shall not exceed the sum of Rs. _____/- (Rupees _____ Only)
- c) Our liability under this agreement shall not be affected by any infirmity or irregularity on the part of our said constituents in tendering for the said work or their obligations there under or by dissolution or change in the constitution of our said constituents.
- d) This guarantee shall remain in force upto 180 days provided that if so desired by the SBI, this guarantee shall be renewed for a further period as may be indicated by them on the same terms and conditions as contained herein.
- e) Our liability under this presents will terminate unless these presents are renewed as provided herein upto 180 days or on the day when our said constituents comply with their obligations, as to which a certificate in writing by the SBI alone is the conclusive proof, whichever date is earlier.
- f) Unless a claim or suit or action is filed against us on or before _____ (date to be filled by BG issuing bank), all the rights of the SBI against us under this guarantee shall be forfeited and we shall be released and discharged from all our obligations and liabilities hereunder.
- g) 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 hereinabove:



- (a) Our liability under this Bank Guarantee shall not exceed Rs...../- (Rupeesonly)
- (b) This Bank Guarantee shall be valid upto
- (c) We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before

Yours faithfully,

For and on behalf of

Authorized official of the bank

(Note: This guarantee will require stamp duty as applicable in the State where it is executed and shall be signed by the official(s) whose signature and authority shall be verified)

Appendix-P

Data Processing Agreement

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 Subprocessors 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 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 30 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 30 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 operational processes with periodic review, including but not limited to:	a. Business Continuity Management	
		b. Backup management	
		c. Desktop/system/server/network device hardening with baseline controls	
		d. Patch Management	

S. No	Controls to be implemented	Compliance (Yes / No)	If under implementation, give date by which implementation will be done
	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?		
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?		

S. No	Controls to be implemented	Compliance (Yes / No)	If under implementation, give date by which implementation will be done
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	
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?		

S. No	Controls to be implemented	Compliance (Yes / No)	If under implementation, give date by which implementation will be done
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)?		
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.		

S. No	Controls to be implemented	Compliance (Yes / No)	If under implementation, give date by which implementation will be done
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. 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	

Engagement of Managed Security Service Provider for
 Cyber Security Defense center (CSDC) under CSCoE in
 bank environment



S. No	Controls to be implemented	Compliance (Yes / No)	If under implementation , give date by which implementation will be done
	including the Law Enforcement Agencies.		