REQUEST FOR PROPOSAL
FOR PROCUREMENT OF
SOFTWARE SOLUTION & SERVICES FOR ENTERPRISE API INTEGRATION AND MANAGEMENT PLATFORM

Ref: SBI/GITC/EIS2.0/2024-25/1221 dated: 14/10/2024

Enterprise Integration Services 2.0
State Bank Global IT Centre,
4th Floor, "A" Wing, Sector-11,
CBD Belapur, Navi Mumbai - 400614

Schedule of Events

Sl No	Particulars	Remarks
1	Contact details of issuing department (Name, Designation, Mobile No., Email and office address for sending any kind of correspondence regarding this RFP)	Name: Sumit Kumar Saha Designation: Chief Manager (IT-EIS 2.0) Email ID: cmit.eis2@sbi.co.in Contact Address: State Bank Global IT Centre, 4th Floor, "A" Wing, Sector-11, CBD Belapur, Navi Mumbai - 400614 Contact Number: +91 22 27537761
2	Bid Document Availability including changes/amendments if any to be issued	RFP may be downloaded from Bank's website https://www.sbi.co.in procurement news from 14/10/2024 to 11/11/2024
3	Last date for requesting clarification	Upto 15.00 hrs on 21/10/2024 All communications regarding points / queries requiring clarifications shall be given in writing or by e-mail.
4	Pre - bid Meeting at (venue)	From 15.00 hrs to 17.00 hrs on 24/10/2024 at SBI Global IT Center, CBD Belapur, Navi Mumbai or any other date as announced/ communicated by the Bank.
5	Clarifications to queries raised at pre-bid meeting will be provided by the Bank.	On 29/10/2024 or any other date as announced/ communicated by the Bank.
6	Last date and time for Bid submission	Upto 15:00 hrs on 11/11/2024 or any other date as announced / communicated by the Bank.
7	Address for submission of Bids *(Please incorporate details of e-Procurement Agency portal wherein online bid has to be submitted)*	Bids to be submitted on the e-tendering portal https://etender.sbi
8	Date and Time of opening of Technical Bids	16.00 hrs on 11/11/2024 or any other date as announced / communicated by the Bank. 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 the Bidder representatives.

9	Opening of Commercial Price Bids	Commercial price bid of technically qualified bidders only will be opened on a subsequent date.
10	Intentionally left blank	
11	Tender Fee	Rs. 25,000.00 (Rupees Twenty-five thousand only) Amount should be deposited in A/c No: 4897932113433 IFSC: SBIN0011343 Account Name: Subsidy Inward Remittance (If Mode of Transaction is NEFT and RTGS) Account No: 37608352111 IFSC: SBIN0011343 Branch: OAD, GITC, Belapur Account Name: System Suspense Branch Parking Account If Mode of Transaction is Intra-bank transfer (i.e. SBI to SBI only) Tender fee will be non-refundable.
12	Earnest Money Deposit	Rs. 2,00,00,000 (Rupees Two-crore only) Amount should be deposited in A/c No: 4897932113433 IFSC: SBIN0011343 Account Name: Subsidy Inward Remittance (If Mode of Transaction is NEFT and RTGS) Account No: 37608352111 IFSC: SBIN0011343 Branch: OAD, GITC, Belapur Account Account Name: System Suspense Branch Parking Account If Mode of Transaction is Intra-bank transfer (i.e. SBI to SBI 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	**5 % of Total Project Cost**	Performance Security in form of BG should be valid for **Five (5)** year(s) and three (3) months from the effective date of the Contract.
14	Contact details of e-Procurement agency appointed for e-procurement	Email ID: etender.support@sbi.co.in Contact Numbers: 7859800621 / 6352631766 / 9081000427	

Contents

SCHEDULE OF EVENTS 2
CONTENTS 5
1. INVITATION TO BID: 11
2. DISCLAIMER: 11
3. DEFINITIONS: 12
4. SCOPE OF WORK: 15
5. ELIGIBILITY AND TECHNICAL CRITERIA: 16
6. COST OF BID DOCUMENT: 16
7. CLARIFICATION AND AMENDMENTS ON RFP/PRE-BID MEETING: 16
8. CONTENTS OF BID DOCUMENT: 17
9. EARNEST MONEY DEPOSIT (EMD): 17
10. BID PREPARATION AND SUBMISSION: 18
11. DEADLINE FOR SUBMISSION OF BIDS: 20
12. MODIFICATION AND WITHDRAWAL OF BIDS: 21
13. PERIOD OF BID VALIDITY 21
14. BID INTEGRITY: 21
15. BIDDING PROCESS/OPENING OF TECHNICAL BIDS: 22
16. TECHNICAL EVALUATION: 22
17. EVALUATION OF COMMERCIAL PRICE BIDS AND FINALIZATION: 23
18. CONTACTING THE BANK: 27
19. AWARD CRITERIA AND AWARD OF CONTRACT: 27
20. POWERS TO VARY OR OMIT WORK: 29
21. WAIVER OF RIGHTS: 29
22. CONTRACT AMENDMENT: 30
23. BANK'S RIGHT TO ACCEPT ANY BID AND TO REJECT ANY OR ALL BIDS: 30
24. BANK GUARANTEE: 30
25. SYSTEM INTEGRATION TESTING & USER ACCEPTANCE TESTING: 30
26. SERVICES: 31
27. WARRANTY AND ANNUAL MAINTENANCE CONTRACT: 31
28. PENALTIES: 33
29. RIGHT TO VERIFICATION: 33
30. INSPECTION AND TESTING: 33
31. RIGHT TO AUDIT: 34
32. SUBCONTRACTING: 35
33. VALIDITY OF AGREEMENT: 35
34. LIMITATION OF LIABILITY: 36
35. CONFIDENTIALITY: 36
36. DELAY IN SERVICE PROVIDER'S PERFORMANCE: 36
37. SERVICE PROVIDER'S OBLIGATIONS: 37
38. TECHNICAL DOCUMENTATION: 38
39. INTELLECTUAL PROPERTY RIGHTS AND OWNERSHIP: 38
40. LIQUIDATED DAMAGES: 40
41. CONFLICT OF INTEREST: 40
42. CODE OF INTEGRITY AND DEBARMENT/BANNING: 42
43. TERMINATION FOR DEFAULT: 45
44. FORCE MAJEURE: 46
45. TERMINATION FOR INSOLVENCY: 46

46. TERMINATION FOR CONVENIENCE: 47
47. DISPUTES RESOLUTION: 47
48. GOVERNING LANGUAGE: 47
49. APPLICABLE LAW: 47
50. TAXES AND DUTIES: 47
51. TAX DEDUCTION AT SOURCE: 49
52. TENDER FEE: 49
53. EXEMPTION OF EMD AND TENDER FEE: 49
54. NOTICES: 50
APPENDIX–A 52
APPENDIX-B 55
APPENDIX-C 59
APPENDIX-D 79
APPENDIX-E 80
E1. CONTEXT AND OBJECTIVES 80
E2. DESCRIPTION OF PRODUCT/SERVICES 81
E3. DESCRIPTION OF DELIVERABLES 104
E4. Third-Party Components 112
E5. Warranty Term 112
E6. Annual Maintenance (AMC) Term 112
E7. MIS Report Generation requirement 116
E8. In case of Transaction System 116
E9. Performance Requirements 116
E10. Scalability Requirements 118
E11. Regulatory / Compliance Requirements 118
E12. Security Requirements 118
E13. Limited Trial / Pilot Requirements 122
E14. Review and Testing; Acceptance 122
E15. Backup system / POC / test & training system / DR system 122
E16. Training 122
APPENDIX-F 124
APPENDIX-G 127
APPENDIX–H 128
APPENDIX-I 131
APPENDIX-J 133
APPENDIX-K 140
APPENDIX-L 216
APPENDIX-M 222
APPENDIX-N 223
APPENDIX-O 224
APPENDIX-P 232
APPENDIX-Q 235
APPENDIX-R 249
APPENDIX-S 253
APPENDIX-T 255
T.1 Platform Capabilities 255
T.2 Bill of Material 282
T.3 Implementation approach 284
T.4 Bidder Evaluation 290

T.5 Tools Demo *291*
T.6 Reference Call and/ or Visit *291*
APPENDIX-U 292
GLOSSARY 293

Part-I

S. N.	INDEX
1	SCHEDULE OF EVENTS
2	INVITATION TO BID
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 COMMERCIALL BID
14	BID INTEGRITY
15	BIDDING PROCESS/ OPENING OF TECHNICAL BIDS
16	TECHNICAL EVALUATION
17	EVALUATION OF COMMERCIAL PRICE BIDS AND FINALIZATION
18	CONTACTING THE BANK
19	AWARD CRITERIA AND AWARD OF CONTRACT
20	POWER TO VARY OR OMIT WORK
21	WAIVER OF RIGHTS
22	CONTRACT AMENDMENT
23	BANK'S RIGHT TO ACCEPT ANY BID AND TO REJECT ANY OR ALL BIDS
24	BANK GUARANTEE
25	SYSTEM INTEGRATION TESTING AND USER ACCEPTANCE TESTING
26	SERVICES
27	WARRANTY AND ANNUAL MAINTENANCE CONTRACT
28	PENALTIES
29	RIGHT TO VERIFICATION
30	INSPECTION AND TESTING
31	RIGHT TO AUDIT
32	SUB-CONTRACTING
33	VALIDITY OF AGREEMENT
34	LIMITATION OF LIABILITY
35	CONFIDENTIALITY
36	DELAY IN SERVICE PROVIDER'S PERFORMANCE

37	SERVICE PROVIDER'S OBLIGATIONS
38	TECHNICAL DOCUMENTATION
39	INTELLECTUAL PROPERTY RIGHTS AND OWNERSHIP
40	LIQUIDATED DAMAGES
41	CONFLICT OF INTEREST
42	CODE OF INTEGRITY AND DEBARMENT/BANNING
43	TERMINATION FOR DEFAULT
44	FORCE MAJEURE
45	TERMINATION FOR INSOLVENCY
46	TERMINATION FOR CONVENIENCE
47	DISPUTES/ARBITRATION
48	GOVERNING LANGUAGES
49	APPLICABLE LAW
50	TAXES AND DUTIES
51	TAX DEDUCTION AT SOURCES
52	TENDER FEE
53	EXEMPTION OF EMD AND TENDER FEE
54	NOTICES

Part-II

APPENDIX	INDEX
A	BID FORM
B	BIDDER'S ELIGIBILITY CRITERIA
C	TECHNICAL & FUNCTIONAL SPECIFICATIONS
D	BIDDER DETAILS
E	SCOPE OF WORK AND PAYMENT SCHEDULE
F	COMMERCIAL PRICE BID
G	CERTIFICATE OF LOCAL CONTENT
H	BANK GUARANTEE FORMAT
I	PROFORMA OF CERTIFICATE TO BE ISSUED BY THE BANK AFTER SUCCESSFUL COMMISSIONING AND ACCEPTANCE OF THE SOFTWARE SOLUTION/ SERVICES
J	PENALTIES
K	SERVICE LEVEL AGREEMENT
L	NON-DISCLOSURE AGREEMENT
M	PRE-BID QUERY FORMAT
N	FORMAT FOR SUBMISSION OF CLIENT REFERENCES
O	PRE-CONTRACT INTEGRITY PACT
P	FORMAT FOR EMD BANK GUARANTEE
Q	DATA PROCESSING AGREEMENT

R	RESOURCE REQUIREMENT
S	MANUFACTURERS' AUTHORIZATION FORM
T	TECHNICAL EVALUATION METRICS
U	PERFORMANCE CERTIFICATE OF OEM

1. INVITATION TO BID:

i. **State Bank of India** (herein after referred to as **'SBI/the Bank')**, having its Corporate Centre at Mumbai, various other offices (LHOs/ Head Offices /Zonal Offices/Global Link Services, Global IT Centre, foreign offices etc.) of State Bank of India, branches/other offices. This Request for Proposal (RFP) has been issued by the Bank on behalf of SBG for procurement, supply, installation, build, integration, designing, development, testing, operation, support and maintenance of Enterprise API Integration and Management Platform for a period of 5 years.

ii. In order to meet the Software Solution/ 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 document.

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

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

v. The purpose of SBI behind this RFP is to seek a detailed technical and commercial proposal for procurement of the Software Solution/ service desired in this RFP. The proposed Software Solution/ service must integrate with Bank's existing infrastructure seamlessly.

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

vii. Interested Bidders are advised to go through the entire RFP before submission of online Bids to avoid any chance of elimination. The eligible Bidders desirous of taking up the project for supply of proposed Software Solution/ service 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 Software Solution/ service adhering to Bank's requirements outlined in this RFP.

2. DISCLAIMER:

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

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

iii. The purpose of this RFP is to provide the Bidder(s) with information to assist preparation of their Bid proposals. This RFP does not claim to contain all the information each Bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information contained in this RFP and where necessary obtain independent advices/clarifications. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

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

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

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

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

3. DEFINITIONS:

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

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

ii. **"Integrated Product Suite**": An **"***Integrated Product Suite***"** including below mentioned major components for deployment of the Enterprise API Integration and Management platform:

Enterprise Service Bus (ESB)

API Gateway

API Management and control

API Orchestration

API Security

Message Queuing Service

Integrated Product Monitoring

Note: "*Platform*" has been referred to as *"Integrated Product Suite"* in this RFP document.

iii. Enterprise Service Bus (ESB) is considered as "Primary Component" for Integrated Product Suite.

iv. OEM of "Primary Component" will be considered as "Primary OEM" hereafter will be referred as "OEM" unless explicitly mentioned. The components which are not from Primary OEM will be considered as 3rd party OEM components. MANUFACTURERS' AUTHORIZATION FORM (MAF) (Appendix-S) will be applicable for both Primary and 3rd Party OEMs.

v. **"Bidder/ Channel Partner / Service Provider"** means an eligible entity/firm submitting the Bid in response to this RFP. A bidder can be:

a. "Primary OEM" OR "Exclusive Distributor in India" OR "Channel Partner".

b. ONLY One channel partner can bid for ONLY one "Primary OEM". "Exclusive Distributor" cannot be front ended by any Channel Partner.

c. If OEM is bidding directly, the OEM can subcontract L1 resources and maximum 30% of L2 resources to its authorized partner(s). L3 and above resources should be provided by the OEM.

d. If bid is submitted by Exclusive Distributor, subcontracting is not permitted.

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

vii. **"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.

viii. **"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.

ix. **"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 TC1 Bidder as per the selection criteria set out in the RFP and to whom notification of award has been given by the Bank.

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

xi. **Annual Maintenance Contract (AMC) -** It would be the annual cost of maintenance of Software Solution / Service.

xii. **Enterprise API Integration and Management Platform** - The proposed integration platform - supply, installation, build, integration, designing, development, testing, operation, support and maintenance of which bids are invited. This will also be referred by "EIS 2.0".

xiii. **Licenses:** Licenses can be either perpetual or for the entire duration of the project (i.e. 5 years). Licenses must be in the name of State Bank of India by OEM.

xiv. **Resource Classification**: All resources for the entire duration of the Project will be classified in three categories L1, L2 and L3 as follows:

Table 3.1 Resource Category

Role / Resource Category	Experience	KRAs
Lead Architect, Team Manager, Project Manager, Program Manager, Product Manager, SMEs, Security expert, Network expert, ops/ Infra expert, Database Administrator, Database Developer, L3 etc. **(herein referred as L3)** <u>From OEM Only</u>	10+ Years	Understand needs and As-Is to define system design and specifications Communicate system requirements to development and QA teams; Act as the IT SPOC between SBI and SI/OEM team for the project Management, engineering and testing best practices; design and lead application architecture; Drive API gateway adoption, ensuring adherence to standards, and coordinating efforts across stakeholders;
Senior Developer/ Designer, Senior Support Engineer, Sr. QA, Tech Lead, Team Lead, Senior Security resource, Senior Network resource, Senior ops/ Infra resource, L2 etc. **(herein referred as L2)**	5+ Years	Address advanced technical problems, perform in-depth diagnostics, and manage API lifecycle tasks such as version control and policy management. Ensure security enforcement, rate limiting, and orchestration, and provide detailed analytics; Program well-designed,

Not exceeding 30% by Channel Partner. Minimum 70% from OEM		testable, efficient code; Execute full lifecycle feature development for Enterprise API Integration and Management Platform; Document, develop and maintain platform functionality; defects/ vulnerabilities fixing etc.
Support engineer, Developer, QA tester, Security engineer, Network engineer, ops/ Infra engineer, L1 etc. **(herein referred as L1)** Can be from Channel Partner	3+ Years	Manage and troubleshoot platform and hosted APIs; Ensure audit and statutory compliance and perform patch installations. track bugs, Develop and execute automation scripts; Monitor platform performance and maintain documentation of recurring issues etc.

4. SCOPE OF WORK:

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

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

i. Service Provider shall ensure that the remote access to the Bank's VPN is performed through a laptop/desktop ("Device") specially allotted for that purpose by the Service Provider and not through any other private or public Device.
ii. Service Provider shall ensure that only its authorized employees/representatives access the Device.
iii. Service Provider shall be required to get the Device hardened/configured as per the Bank's prevailing standards and policy.
iv. Service Provider and/or its employee/representative shall be required to furnish an undertaking and/or information security declaration on the Bank's prescribed format before such remote access is provided by the Bank.
v. Service Provider shall ensure that services are performed in a physically protected and secure environment which ensures confidentiality and integrity of the Bank's data and artefacts, including but not limited to information (on customer, account, transactions, users, usage, staff, etc.), architecture (information, data, network, application, security, etc.), programming codes, access configurations, parameter settings, executable files, etc., which the Bank representative may inspect. Service Provider shall facilitate and/ or handover the Device to the Bank or its authorized representative for investigation and/or forensic audit.
vi. Service Provider shall be responsible for protecting its network and subnetworks, from which remote access to the Bank's network is performed, effectively against unauthorized access, malware, malicious code and other threats in order to ensure

the Bank's information technology system is not compromised in the course of using remote access facility.

5. ELIGIBILITY AND TECHNICAL CRITERIA:

i. Bid is open to all Bidders who meet the eligibility and technical criteria as given in Appendix-B & Appendix-C of this document. The Bidder has to submit the documents substantiating eligibility criteria as mentioned in this RFP document.
   a. If any Bidder submits Bid on behalf of Principal/OEM, the same Bidder shall not submit a Bid on behalf of another Principal/OEM under the RFP.
   b. Either the Bidder on behalf of Principal/OEM or Principal/OEM itself is allowed to Bid, however both cannot Bid simultaneously.

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

6. COST OF BID DOCUMENT:

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

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

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

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

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

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

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

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

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

8. CONTENTS OF BID DOCUMENT:

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

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

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

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

9. EARNEST MONEY DEPOSIT (EMD):

i. 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 or it should be in form of Bank Guarantee (as prescribed in **Appendix-P**) issued in favour of State

Bank of India by any scheduled commercial bank in India. In case, SBI is the sole banker of the Bidder, a Letter of Comfort from SBI would be acceptable.

a. 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: -

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

(b) Intentionally left blank

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

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

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.

10. BID PREPARATION AND SUBMISSION:

i. The Bid is to be submitted separately for technical and Price on portal of e-Procurement agency for supply, installation, build, integration, designing, development, testing, operation, support and maintenance of Enterprise API Integration and Management Platform in response to the **RFP No. SBI/GITC/EIS2.0/2024-25/1221 dated 14/10/2024.** 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 (if directly credited in designated account) and Tender Fee as specified in this document. In case, EMD is submitted in form of BG, scanned copy of original BG should be uploaded subject to compliance of requirement mentioned in clause no 11"*DEADLINE FOR SUBMISSION OF BIDS*" sub-clause (ii).

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

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

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

(g) Format for Manufacturer's Authorization Form as per **Appendix-S. Bidder must arrange to submit this form duly signed by the OEM. If the Bidder proposes software / application / tool from 3rd party OEM, Appendix-S is required to be submitted for all such 3rd party OEMs.**

(h) 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.

(i) 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).

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

ii. Commercial Price Bid for supply, installation, build, integration, designing, development, testing, operation, support and maintenance of Enterprise API Integration and Management Platform in response to the RFP No. SBI/GITC/EIS2.0/2024-25/1221 dated 14/10/2024 should contain only Commercial Price Bid strictly on the lines of Appendix-F. The Commercial 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 Commercial Price Bid) is received.

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

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

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

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

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

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

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

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

11. DEADLINE FOR SUBMISSION OF BIDS:

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

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

iii. In 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.

iv. Any Bid received after the deadline for submission of Bids prescribed, will be rejected and returned unopened to the Bidder.

12. MODIFICATION AND WITHDRAWAL OF BIDS:

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

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

iii. No Bid shall be withdrawn in the interval between the deadline for submission of Bids and the expiration of the period of Bid validity specified in this RFP. Withdrawal of a Bid during this interval may result in the forfeiture of EMD submitted by the Bidder.

13. PERIOD OF BID VALIDITY

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

~~ii.~~ Intentionally left blank.

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.

14. BID INTEGRITY:

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

15. BIDDING PROCESS/OPENING OF TECHNICAL BIDS:

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

ii. In the first stage, only technical Bid will be opened and evaluated. Bids of such Bidders satisfying eligibility criteria and agree to comply with all the terms and conditions specified in the RFP will be evaluated for technical criteria/specifications/eligibility. Only those Bids complied with technical criteria shall become eligible for Commercial 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 Software Solution/service proposed to be offered by them.

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

16. TECHNICAL EVALUATION:

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

ii. During evaluation and comparison of Bids, the Bank may, at its discretion ask the Bidders for clarification on the Bids received. The request for clarification shall be

in writing and no change in prices or substance of the Bid shall be sought, offered or permitted. No clarification at the initiative of the Bidder shall be entertained after bid submission date.

17. EVALUATION OF COMMERCIAL PRICE BIDS AND FINALIZATION:

Criteria for Technical Evaluation and Commercial Evaluation

(Techno Commercial evaluation will be used under this RFP. The RFP shall specify the minimum qualifying score for the technical bid and the relative weightages to be given to the technical criteria (quality) and the cost.)

The Criteria for Technical Evaluation and Commercial Evaluation will have weightage of **80:20**.

Bidders scoring **less than 75% marks** in the Technical Evaluation will not be considered for the selection process, and their Commercial Bids will not be opened.

The proposal with the Highest Weighted Combined Score (quality and cost / **TC1**) shall be selected.

In case of tie between two or more bidders for the Highest Total Combined Score, then the bidder with **Highest Technical Score** amongst such bidders shall be the successful bidder.

Illustration:

i. Bids will be evaluated as per Combined Quality Cum Cost Based System. The Technical Bids will be allotted weightage of 80**%** while Commercial Bids will be allotted weightage of 20**%**.

ii. A combined score "**Score (S)"** will be arrived at after considering the Commercial quote and the marks obtained in Technical evaluation with relative weights of 20 **%** for Commercial bid and **80%** for Technical Bid according to the following formula:

$$\textbf{Combined Score of A} = 80 \times \frac{\textbf{Technical Bid Score of A}}{\textbf{Highest Technical Score}} + 20 \times \frac{\textbf{Lowest Commercial Bid}}{\textbf{Commercial Bid of A}}$$

The bidder obtaining the Highest Total Combined Score in evaluation of technical and commercial evaluation will be ranked **TC – 1** followed by proposal securing lesser marks as **TC – 2, TC – 3** etc. **Bidder securing Highest Combined Marks and ranked TC – 1 shall be recommended for award of contract.** Bank will follow the internal procedure for necessary approvals and thereafter proceed with notification of award of contract.

Sr. No	Bidder	Technical Evaluation Marks (t)	Commercial Bid (f)	Weighted technical Score ={(t)/t highest}× 80	Weighted Commercial Score =(f lowest / f) × 20	Score "S" out of 100

1	A	90	60	(90/90) × 80 = 80	(50/60)×20 = 16.67	**96.67**
2	B	80	70	(80/90) × 80 = 71.11	(50/70)×20 = 14.29	**85.40**
3	C	70	50	(70/90) × 80 = 62.22	(50/50)×20 = 20	**82.22**

In the above example, "A" the bidder with the highest score becomes the successful bidder (TC-1).

Final Evaluation:

The commercials will be finalized among the shortlisted bidders who obtain **<75>% or more marks in technical evaluation.** The Final bidder will be selected on the basis of **TC -1** as given above. The bidder securing highest combined marks (Technical score + Commercial score) and ranked **TC-1** shall be recommended for award of contract.

- **Technical Evaluation Score (TES)**

Table: TES-1 Technical Evaluation Score

No	Evaluation Category	Table	Max Score	Weightage %
1	Platform Capabilities	TES 1.1	100	42
2	Bill of Materials	TES 1.2	100	8
3	Implementation approach	TES 1.3	100	11
4	Bidder evaluation	TES 1.4	100	19
5	Tool Demo	TES 1.5	100	12
6	Reference Visit/Call	TES 1.6	100	8
			Total Evaluation Weightage	100

The Total Evaluation Weightage of **100** will be converted to 80% for scoring under TC1.

1.1 Platform Capabilities (Weightage – 42%)

Table: TES-1.1 Platform Capabilities

Dimensions	Themes	Max Score
Feature Coverage	(1) API Design	5
	(2) API Implementation	5
	(3) API Integration	10
	(4) API Governance	5
	(5) API Observability	5
	(6) API Monitoring	5
	(7) API Commercialization	5
	(8) API Publishing	5
	Sub Total	**45**
Technical Capabilities	(9) Messaging	5
	(10) Deployment	5
	(11) Scalability	5
	(12) Latency	5

	(13) Architecture	5
	(14) Security	5
	(15) Third-Party Integrations	15
	(16) Compliance with Standards and Regulations	5
	(17) Portability	5
	Sub Total	**55**
	Total	**100**

1.2 Bill of Materials (Weightage – 8%)

Table: TES-1.2 Bill of Materials

Dimensions	Themes	Max Score
Bill of Materials	Infrastructure Sizing	20
	Applications/software/products	50
	Team construct (Team size, experience, technical qualification)	30
	Total	**100**

1.3 Implementation approach (Weightage – 11%)

Table: TES-1.3 Implementation approach

Dimensions	Themes	Max Score
Planning	Approach	10
	Implementation Plan	10
	Agility	10
	Sub Total	**30**
Delivery	Quality Assurance	15
	Training	5
	Documentation	10
	Compliance	10
	Sub Total	**40**
Support	Enterprise Support	10
	Online Resources and Community	5
	System Integrator Support Capabilities	5
	India-based Product Support	10
	Sub Total	**30**
	Total	**100**

1.4 Bidder evaluation (Weightage – 19%)

Table: TES-1.4 Bidder evaluation

Dimensions	Themes	Max Score
	Partnerships	45

Bidder evaluation	Portfolio and References	30
	Ecosystem Knowledge	25
	Total	**100**

1.5 Tool Demo (Weightage – 12%)

Table: TES-1.5 Tool Demo

Dimensions	Themes	Max Score
Tool Demo	Scope Understanding	10
	Proposed approach and roadmap	20
	Team structure	20
	Relevant case studies	20
	Partnerships with key OEMs	10
	Existing know-how, reusable components, boilerplate code that can be deployed for the bank	10
	Foreseen risks and mitigation approach	10
	Total	**100**

1.6 Reference Visit/Call (Weightage – 8%)

Table: TES-1.6 Reference Visit/ Call

Dimensions	Themes	Max Score
Reference Call and/ or Visit	Reference Size and Scope	20
	Reference technology architecture	30
	Implementation approach including MVP, timelines, agile methodology	30
	Adherence to regulatory compliance, security, risk and other mandatory requirements	20
	Total	**100**

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

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

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

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

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

18. CONTACTING THE BANK:

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

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

19. AWARD CRITERIA AND AWARD OF CONTRACT:

i. <u>Applicability of Preference to Make in India, Order 2017 (PPP-MII Order)</u>

Guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order) and any revision thereto will be applicable for this RFP and only Class-I and Class-II local supplier are allowed to participate in this RFP. As the evaluation of successful bidder is on the basis of TC1, margin of purchase preference to Class-I local supplier shall not be applicable under this RFP.

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.

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 Software Solution 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 Commercial price bid.

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

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

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

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

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

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

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

xi. Upon notification of award to the successful Bidder, the Bank will promptly notify the award of contract to the successful Bidder on the Bank's website. The EMD of each unsuccessful Bidder will be discharged and returned.

20. POWERS TO VARY OR OMIT WORK:

i. No alterations, amendments, omissions, additions, suspensions or variations of the work (hereinafter referred to as variation) under the contract shall be made by the successful Bidder except as directed in writing by Bank. The Bank shall have full powers, subject to the provision herein after contained, from time to time during the execution of the contract, by notice in writing to instruct the successful Bidder to make any variation without prejudice to the contract. The finally selected Bidder shall carry out such variation and be bound by the same conditions as far as applicable as though the said variations occurred in the contract documents. If any, suggested variations would, in the opinion of the finally selected Bidder, if carried out, prevent him from fulfilling any of his obligations under the contract, he shall notify Bank thereof in writing with reasons for holding such opinion and Bank shall instruct the successful Bidder to make such other modified variation without prejudice to the contract. The finally selected Bidder shall carry out such variation and be bound by the same conditions as far as applicable as though the said variations occurred in the contract documents. If the Bank confirms its instructions, the successful Bidder's obligations shall be modified to such an extent as may be mutually agreed, if such variation involves extra cost. Any agreed difference in cost occasioned by such variation shall be added to or deducted from the contract price as the case may be.

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

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

21. WAIVER OF RIGHTS:

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

hereunder on one occasion will not be construed as a bar to a waiver of any successive or other right, power or remedy on any other occasion.

22. CONTRACT AMENDMENT:

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

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

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

24. BANK GUARANTEE:

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

ii. The Bank Guarantee is required to protect the interest of the Bank against delay in supply/installation and/or the risk of non-performance of the successful Bidder in respect successful implementation of the project, or performance of the material or services sold, or breach of any terms and conditions of the Agreement, which may warrant invoking of Bank Guarantee.

25. SYSTEM INTEGRATION TESTING & USER ACCEPTANCE TESTING:

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

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

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

26. SERVICES:

i. All professional services necessary to successfully implement the proposed Software Solution will be part of the RFP/Contract.

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

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

iv. The bidder should ensure that the quality of methodologies for delivering the services adhere to quality standards/timelines stipulated, therefore.

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

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

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

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

ix. All product updates, upgrades & patches shall be provided by the Bidder/ Service Provider free of cost during warranty and AMC/ ATS/ S&S period.

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

xi. The Bidder shall keep the Bank explicitly informed the end of support dates on related products/hardware/firmware and should ensure support during warranty and AMC/ATS/S&S.

27. WARRANTY AND ANNUAL MAINTENANCE CONTRACT:

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

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

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

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

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

vi. Support (Warranty/ AMC, if included in the RFP) would be on-site and comprehensive in nature and must have back-to-back support from the OEM/Service Provider. Undertaking on the lines of **Appendix-S** of this RFP document is required to be submitted by Service Provider, duly endorsed by the Primary OEM and 3rd party OEMs that in case Service Provider fails to provide Services then Primary OEM and 3rd party OEMs shall provide the same at no extra cost, to the satisfaction of the Bank. Service Provider warrants Products against defect arising out of faulty design, materials, etc. during the specified support period. Service Provider will provide support for operating systems and other pre-installed software components/system software during the specified period of the hardware on which these software and operating system will be installed. Service Provider shall repair or replace worn out

or defective parts including all plastic parts of the Equipment at his own cost including the cost of transport.

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

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

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

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

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

28. PENALTIES:

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

29. RIGHT TO VERIFICATION:

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

30. INSPECTION AND TESTING:

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

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

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

(b) The inspection and acceptance test may also be conducted at the point of delivery and / or at the products' final destination. Reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors, at no charge to the Bank. In case of failure by Service Provider to

provide necessary facility / equipment at its premises, all the cost of such inspection like travel, boarding, lodging & other incidental expenses of the Bank's representatives to be borne by Service Provider.

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

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

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

31. RIGHT TO AUDIT:

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

32. SUBCONTRACTING:

i. Sub-Contracting is not permitted. However, Bank may permit sub-contracting on case-to case basis at the sole discretion of the Bank. If permitted, the Service Provider shall carry out its standard due diligence process on sub-contracting/ sub-contractor.
ii. Service Provider shall comply with all the instructions, requirements and any other conditions suggested by the Bank in order for the Bank to comply with its site access and regulatory audit requirements and upon' s Bank request Service Provider will provide a written confirmation of compliance with the requirements of this provision.
iii. With the Bank's prior written approval, Service Provider may change the sub-contractor, provided it does not impact the quality of Services being delivered. However, Service Provider shall inform the Bank on its intention to change the sub-contractor and reason thereof.
iv. Service Provider shall be responsible for all the Services provided to the Bank regardless of which entity is conducting the operations. Service Provider is also responsible for ensuring that the sub-contractor comply with all security/confidentiality requirements and other terms and conditions as applicable to Service Provider mentioned in this RFP. Bank reserves the right to conduct independent audit in this regard.
v. Service Provider shall ensure that suitable documents including confidentiality agreement are obtained from the sub-contractor and the Service Provider shall ensure that the secrecy and faith of the Bank's data / processes is maintained.
vi. Notwithstanding approval of the Bank for sub-contracting, the Service Provider shall remain liable to the Bank for all acts/omissions of sub-contractors.
vii. Service Provider shall ensure that it shall have all back-to-back commitments from its vendors in such agreements.
viii. Service Provider shall provide the complete details of Services sub-contracted by it including the details of sub-contractor(s) and/or its agent to the Bank as and when requested.

33. VALIDITY OF AGREEMENT:

The Agreement/ SLA will be valid for the period of Five (5) year(s). The Bank reserves the right to terminate the Agreement as per the terms of RFP/ Agreement.

34. LIMITATION OF LIABILITY:

i. The maximum aggregate liability of Service Provider, subject to 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.

35. CONFIDENTIALITY:

Confidentiality obligation shall be as per Non-disclosure agreement and clause 15 of Service Level Agreement placed as Appendix to this RFP.

36. DELAY IN SERVICE PROVIDER'S PERFORMANCE:

i. Delivery, installation, commissioning of the Software Solution and performance of Services shall be made by Service Provider within the timelines prescribed in Part II of this RFP.

ii. If at any time during performance of the Contract, Service Provider should encounter conditions impeding timely delivery of the Software Solution and performance of

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

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

37. SERVICE PROVIDER'S OBLIGATIONS:

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

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

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

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

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-L** 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-Q 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.

38. TECHNICAL DOCUMENTATION:

i. Service Provider shall deliver the following documents to the Bank for every software including third party software before software/ service become operational, which includes, user manuals, installation manuals, operation manuals, design documents, process documents, technical manuals, functional specification, software requirement specification, on-line tutorials/ CBTs, system configuration documents, system/database administrative documents, debugging/diagnostics documents, test procedures etc.

ii. Service Provider shall also provide documents related to Review Records/ Test Bug Reports/ Root Cause Analysis Report, list of all Product components, list of all dependent/external modules and list of all documents relating to traceability of the Software Solution as and when applicable.

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

39. INTELLECTUAL PROPERTY RIGHTS AND OWNERSHIP:

i. For any technology / Software / solution developed/used/supplied by Service Provider for performing Services or licensing and implementing Software and solution for the Bank as part of this RFP, Service Provider shall have right to use as well right to license for the outsourced services or third party 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 cost, 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 use of the technology / Software / products or any part thereof in India or abroad, for Software licensed/developed as part of this engagement. In case of violation/ infringement of patent/ trademark/ copyright/ trade secret or industrial design or any other Intellectual Property Right of third party, Service Provider shall, after due inspection and testing, without any additional cost (a) procure for the Bank the right to continue to using the Software supplied; or (b) replace or modify the Software to make it non-infringing so long as the replacement to or modification of Software provide substantially equivalent functional, performance and operational features as the infringing Software which is being replaced or modified; or (c) to the extent that the activities under clauses (a) and (b) above are not commercially reasonable, refund to the Bank all amounts paid by the Bank to Service Provider under this RFP/Agreement.

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

v. Service Provider shall have no obligations with respect to any infringement claims to the extent that the infringement claim arises or results from: (i) Service Provider's compliance with the Bank's specific technical designs or instructions (except where Service Provider knew or should have known that such compliance was likely to result in an infringement claim and Service Provider did not inform the Bank of the same); (ii) any unauthorized modification or alteration of the Software by the Bank or its employee; (iii) failure to implement an update to the licensed software that would have avoided the infringement, provided Service Provider has notified the Bank in writing that use of the update would have avoided the claim.

vi. Service Provider shall grant the Bank a fully paid-up, irrevocable, exclusive, unlimited, perpetual license throughout the territory of India or abroad to access, replicate and use software provided by Service Provider, including all inventions, designs and marks embodied therein perpetually. The source code, object code, executable code and compilation procedures of the Software Solution over and above the OEM products, made under this agreement, are the proprietary property of the Bank and as such Service Provider shall make them available to the Bank after successful User Acceptance Testing. 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. This also includes architecture design, network design, infrastructure design, integration design etc. implemented at SBI. Any work made under this agreement shall be deemed to be 'work made for hire' under any Indian/U.S. or any other applicable copyright laws.

40. LIQUIDATED DAMAGES:

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

41. CONFLICT OF INTEREST:

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

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

(a) the Bidder, its Member or Associate (or any constituent thereof) and any other Bidder, its Member or any Associate thereof (or any constituent thereof) have common controlling shareholders or other ownership interest; provided that this

disqualification shall not apply in cases where the direct or indirect shareholding of a Bidder, its Member or an Associate thereof (or any shareholder thereof having a shareholding of more than 5% (five per cent) of the paid up and subscribed share capital of such Bidder, Member or Associate, as the case may be) in the other Bidder, its Member or Associate, has less than 5% (five per cent) of the subscribed and paid up equity share capital thereof; provided further that this disqualification shall not apply to any ownership by a bank, insurance company, pension fund or a public financial institution referred to in section 2(72) of the Companies Act, 2013. For the purposes of this Clause, indirect shareholding held through one or more intermediate persons shall be computed as follows: (aa) where any intermediary is controlled by a person through management control or otherwise, the entire shareholding held by such controlled intermediary in any other person (the "Subject Person") shall be taken into account for computing the shareholding of such controlling person in the Subject Person; and (bb) subject always to sub-clause (aa) above, where a person does not exercise control over an intermediary, which has shareholding in the Subject Person, the computation of indirect shareholding of such person in the Subject Person shall be undertaken on a proportionate basis; provided, however, that no such shareholding shall be reckoned under this sub-clause (bb) if the shareholding of such person in the intermediary is less than 26% of the subscribed and paid up equity shareholding of such intermediary; or

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

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

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

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

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

iii. For the purposes of this RFP, Associate means, in relation to the Bidder, a person who controls, is controlled by, or is under the common control with such Bidder (the "Associate"). As used in this definition, the expression "control" means, with respect to a person which is a company or corporation, the ownership, directly or indirectly,

of more than 50% (fifty per cent) of the voting shares of such person, and with respect to a person which is not a company or corporation, the power to direct the management and policies of such person by operation of law or by contract.

42. CODE OF INTEGRITY AND DEBARMENT/BANNING:

i. The Bidder and their respective officers, employees, agents and advisers shall observe the highest standard of ethics during the bidding Process. Notwithstanding anything to the contrary contained herein, the Bank shall reject Bid without being liable in any manner whatsoever to the Bidder if it determines that the Bidder has, directly or indirectly or through an agent, engaged in corrupt/fraudulent/coercive/undesirable or restrictive practices in the bidding Process.

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

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

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

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

(b) **"Fraudulent practice"** means any omission or misrepresentation that may mislead or attempt to mislead so that financial or other benefits may be obtained or an obligation avoided. This includes making false declaration or providing false information for participation in 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

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

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

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

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

(b) Debarment from participation including removal from empaneled list

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

- Without prejudice to the rights of the Bank under Clause *42" 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.

43. TERMINATION FOR DEFAULT:

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

(a) If the 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 the 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, software and 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 Software Solution and/or 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 or in case of software provision for future upgrades.

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 the Service Provider to render the Services or in the event of termination of Agreement or expiry of term or otherwise, without prejudice to any other right, the Bank at its sole discretion may make alternate arrangement for getting the Services contracted with another vendor. In such case, the Bank shall give prior

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

44. FORCE MAJEURE:

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

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

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

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

45. TERMINATION FOR INSOLVENCY:

The Bank may, at any time, terminate the Contract by giving written notice to Service Provider, if Service Provider becomes Bankrupt or insolvent or any application for bankruptcy, insolvency or winding up has been filed against it by any person. In this

event, termination will be without compensation to Service Provider, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to the Bank.

46. TERMINATION FOR CONVENIENCE:

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

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

47. DISPUTES 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.

48. GOVERNING LANGUAGE:

The governing language shall be English.

49. APPLICABLE LAW:

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

50. TAXES AND DUTIES:

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

ii. Prices quoted should be exclusive of 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.

51. TAX DEDUCTION AT SOURCE:

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

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

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

52. TENDER FEE:

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

53. EXEMPTION OF EMD AND TENDER FEE:

Micro & Small Enterprises (MSE) units and Start-ups* are exempted from payment of EMD and tender fee provided the products and/or services they are offering, are

manufactured and/or services rendered by them. Exemption as stated above is not applicable for selling products and/or services, manufactured/ 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.

54. NOTICES:

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

Part-II

Appendix–A

BID FORM (TECHNICAL BID)

[On Company's letter head]

(To be included in Technical Bid)

Date: _____

To:

< Address of tendering office >

Dear Sir,

Ref: RFP No. SBI/GITC/EIS2.0/2024-25/1221 dated 14/10/2024

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 supply, install, build, integrate, design, develop, test, operate, support and maintain the desired Software Solution 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 eTender Portal to be conducted by the Bank's authorized service provider, on the date advised to us.

1. While submitting this Bid, we certify that:
    1. The undersigned is authorized to sign on behalf of the Bidder and the necessary support document delegating this authority is enclosed to this letter.
    2. We declare that we are not in contravention of conflict of interest obligation mentioned in this RFP.
    3. Commercial prices submitted by us have been arrived at without agreement with any other Bidder of this RFP for the purpose of restricting competition.
    4. The Commercial prices submitted by us have not been disclosed and will not be disclosed to any other Bidder responding to this RFP.
    5. We have not induced or attempted to induce any other Bidder to submit or not to submit a Bid for restricting competition.
    6. We have quoted for all the products/services mentioned in this RFP in our Commercial price Bid.
    7. The rate quoted in the Commercial price Bids are as per the RFP and subsequent pre-Bid clarifications/ modifications/ revisions furnished by the Bank, without any exception.
2. 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".

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

4. 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.

5. 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.

6. 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.

7. We agree to abide by all the RFP terms and conditions, contents of Service Level Agreement as per template available at **Appendix-K** 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.

8. Intentionally left blank

9. Intentionally left blank

10. 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.

11. 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.

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

13. 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.

14. We hereby certify that we (participating in RFP as OEM)/ our OEM have a support center and level 3 escalation (highest) located in India.

15. 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.

16. 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.

17. 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.

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

Dated this ..... day of ..... 20..

_____

(Signature) *(Name)*

(In the capacity of)

Duly authorised to sign Bid for and on behalf of

_____**Seal of the company.**

Appendix-B

Bidder's Eligibility Criteria

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

S. No	Eligibility Criteria	Compliance (Yes/No)	Documents to be submitted
1.	The Bidder must be an Indian Company/ LLP /Partnership firm registered under applicable Act in India.		Certificate of Incorporation issued by Registrar of Companies and full address of the registered office along with Memorandum & Articles of Association/ Partnership Deed.
2.	The Bidder (including its OEM, if any) must comply with the requirements contained in O.M. No. 6/18/2019-PPD, dated 23.07.2020 order (Public Procurement No. 1), order (Public Procurement No. 2) dated 23.07.2020 and order (Public Procurement No. 3) dated 24.07.2020		Bidder should specifically certify in **Appendix-A** in this regard and provide copy of registration certificate issued by competent authority wherever applicable.
3.	The Bidder must have an average turnover of minimum Rs. **250** crore during last 03 (three) financial year(s) i.e. FY 2021-22, FY2022-23 and FY 2023-24. This must be the individual company's average turnover and not of any group of companies.		Copy of the audited financial statement for required financial years.
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	The bidder should have experience of minimum 3 years as on 30.09.2024 in providing solution / services which includes installation, development, implementation and operation/maintenance of similar projects in BFSI sector (Banking, Financial Services and Insurance) in India.		Relevant copy of Purchase Order/SLA along with any one of the following should be submitted: • Completion certificates • Project Sign-offs • Satisfactory client certificates
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.	**Proposed Integrated Product Suite of OEM:** The "Integrated Product Suite" (please refer Definition section for "Integrated Product Suite") proposed in the bid should be currently in use by minimum 2 BFSI clients in India and minimum 2 BFSI clients in abroad as on 30.09.2024.		Relevant project completion documents along with satisfactory sign-offs by the client as per **Appendix-U**.
8.	**Integrated Product Suite Implementation by the Bidder:** Client references and contact details (email/ landline/ mobile) of customers for whom the **Bidder** has executed (as on 30.09.2024) similar projects (minimum 2 clients) in India using the OEM's Integrated Product Suite quoted in this bid.		Bidder should specifically confirm on their letter head in this regard as per **Appendix-N**
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, 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.
12	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.

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 S.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:

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.

Bidder who solely on its own, fulfils each eligibility criteria condition as per the RFP terms and conditions and who are having Start-up company status, can claim exemption for eligibility criteria mentioned at Sl No 3 to 5 in table above.

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 authorised signatory

Seal of Company

Appendix-C

Technical & Functional Specifications

Technical Capabilities and the components that are required for Enterprise API Integration and Management Platform (EIS 2.0) are as follows, however this is a non-exhaustive list:

Bidder response to Technical Specifications

The bidder is expected to respond to the platform capabilities by mentioning the mode of availability **(Complied Flag)** of the specific capability (mentioned in the table below), along with supporting documentation mentioning clear feature details and explanation related to the option chosen, in terms of native or third-party availability.

Table C-1 Mode of Availability

S. No.	Complied Flag	Parameter Value	Description
1	A	Available out-of-the-box	Available as part of bidder's proposed solution from OEM (native or configured)
2	B	Available with customization	Available as part of bidder's proposed solution from OEM (but requires customization (managed by the bidder)
3	C	Functionality already implemented through 3rd Party tool/ software	Available as part of an integrated 3rd party solution (managed by bidder), costs included in the bid
4	D	Functionality compatible to be implemented through 3rd party tool/ software	Potential third-party providers indicated, bidder is responsible for integrating
5	E	Not available or not provided	Not available as part of proposed solution

Note: Response to all items in the below table is mandatory

1. **API Design-**

The process of designing the APIs that expose data and application functionality for use by developers and users.

Table C-2 API Design

S no	Requirements	Requirement Type	Complied Flag (A/B/C/D/E)	OEM/ Product/ Module Name
1	The platform should support **async API design and documentation**.	Mandatory		

2	The platform should have **clear segregation** of System, Process and Experience layer.	Mandatory		
3	The platform should provide support for design artefacts such as **OAS (OpenAPI Specification), RAML (RESTful API Modelling Language)** standards etc.	Mandatory		
4	The platform should be capable of fetching **design data from 3rd party API design** tools in Swagger	Mandatory		
5	The platform should be able to parse and **validate the structure of API specification** files against the schema of the specification language	Mandatory		
6	The platform must have **readymade patterns** for common API design patterns, such as **pagination, filtering, and sorting** available	Mandatory		
7	The platform must provide the capability of **customization of components**, such as API endpoints or data models	Mandatory		
8	The platform should enable support for **response callback APIs**, to manage asynchronous API flows	Mandatory		
9	The platform must provide an **Integrated Development Environment (IDE**) with tools and features for API development, testing, and debugging	Mandatory		
10	The platform should enable **integration with Gen AI** tools for API design	Essential		
11	The platform should provide an **OOTB (Out of the Box) web based and desktop-based platform** for supporting design of APIs	Essential		
12	The platform should enable **automation of decision processes** and services like document recognition.	Optional		

2. **API Implementation-**

API Management Platform will lie at the heart of the EIS 2.0 layer. The platform will develop and maintain orchestrated APIs that serve as an exchange medium between the customer facing channels such as YONO, RINB, FIGS etc. and the core systems such as CBS, LLMS etc. and databases. The platform will provide a one-stop solution for all types of API development needs starting from designing a new API from scratch to making minor and major modifications to existing APIs.

Table C-3 API Implementation

S no	Requirements	Requirement Type	Complied Flag (A/B/C/D/E)	OEM/ Product/ Module Name
1	The platform should provide support for **event streaming** (Kafka, Solace, AWS Kinesis, Azure EventHub etc.) and **queuing platforms**	Mandatory		
2	The platform would support processing of **business rules for transactions** and corresponding routing	Mandatory		
3	The platform components should have the capability to deliver **bank specific customizations** in quick time	Mandatory		
4	The platform should provide **drag and drop functionality**, to allow developers to easily create and configure APIs by visually arranging components or modules	Mandatory		
5	The platform should have **low-code no-code features**, Desktop based and web-based IDE.	Mandatory		
6	The platform should have simplified **developer portal & API catalogue.**	Mandatory		
7	The platform must provide an **out of the Box developer portal** with pre-built themes and templates, along with the ability to customize the portal with low code, along with **self on-boarding with customized workflow** with consumption metrics.	Mandatory		
8	The platform should support **plug & play for Java code.**.	Mandatory		
9	Error code and messages design mapping: Platform to provide and handle **error code and messages design** mapping customizations.	Mandatory		
10	The platform should support multiple data transport protocols such as **SOAP, HTTP, REST, File, JDBC (Java Database Connectivity)**	Mandatory		
11	The platform must be compatible with multiple data formats to cover **JSON, CSV and XML files** etc.	Mandatory		
12	The platform should provide support for existing **CI/CD pipeline** for automated build, test, and deployment processes.	Mandatory		

13	The platform should enable **hosting of virtual APIs** with 24/7 access to API playground.	Mandatory		
14	The platform should enable **simulation of issues and edge cases** to support load testing, regression testing and performance testing	Mandatory		
15	The platform should provide **packaging support** for API to convert into a **deployable JAR or ZIP file**	Mandatory		
16	The platform should enable **direct application of rate limiting and throttling policies** directly to APIs	Mandatory		
17	The platform should **Circuit breaker functionality** to handle and recover from failures in distributed systems, preventing cascading failures	Mandatory		
18	The platform should enforce **load balancing mechanisms** to distribute incoming requests across multiple instances (instances activated through cloud service configuration)	Mandatory		
19	The platform should support **high throughput capabilities** to handle a large volume of requests or transactions	Mandatory		
20	The platform should ensure **sanitization of user input** to prevent security vulnerabilities such as **SQL injection or cross-site scripting attacks**	Mandatory		
21	The platform should provide **conducive implementation language support** and less dependency on proprietary technologies like Java, .NET, etc.	Essential		
22	The platform should have **complete auto configuration** of all components.	Essential		
23	The platform should provide **testing framework support** for **Junit and others** for automated testing of APIs.	Essential		
24	The platform to provide an **automatic API service discovery layer**	Essential		
25	The platform should support **AI(GPT/LLM) based prompts** to generate integration flows to improve developer productivity.	Optional		

3. **API Integration**-
The process of connecting two or more applications or systems by using APIs to exchange data and perform actions.

Table C-4 API Integration

S no	Requirements	Requirement Type	Complied Flag (A/B/C/D/E)	OEM/ Product/ Module Name
1	The platform should be able to **route API messages** to multiple downstream applications extensively.	Mandatory		
2	The platform should be able to **transform the messages** between multiple data formats	Mandatory		
3	The platform should have **ESB and messaging components** to support interoperability among different applications. different channels, downstream service providers, external integrations, and existing EIS.	Mandatory		
4	The platform should support all relevant data formats e.g. **JSON, XML, Strings, Text, CSV, Flat File format, Fixed Width format, COBOL, JSON, YAML, Custom Type, Excel etc.**	Mandatory		
5	The platform should support **multiple data type support** including BLOB.	Mandatory		
6	The platform should support multiple transport protocols such as **SOAP & Webservices, JMS, HTTP, RESTful, File, Websocket, , JDBC, TCP/UDP Socket, OData, SFTP & FTPS, ISO Base24 Fix length etc.**	Mandatory		
7	The platform should support **UDDI specification to publish and discover information** about web services.	Mandatory		
8	The platform should have the **capability to convert one protocol to another protocol**.	Mandatory		
9	The platform to have **out-of-the-box connector** to connect to **downstream applications like CBS, RLMS**, etc.	Mandatory		
10	The platform should have the ability to integrate with **existing governance platform** of the Bank. e.g. **PIMS, SIEM, DAM**, etc.	Mandatory		
11	The platform should provide the flexibility to build **custom connectors with SDK**.SDK for **custom API policies**.	Mandatory		

12	The platform should have readymade palette for integration with **JDBC , FTP, SFTP, TCP** etc.	Mandatory		
13	The platform should provide support for **unit testing** and code coverage.	Mandatory		
14	Exposed APIs should be compatible for any **internal systems for ease of integration** (built as RESTful)	Mandatory		
15	Integration support with **external monitoring platforms** to provide health status of services.	Mandatory		
16	API Validation/simulation	Mandatory		
17	The platform should have the capability of **decision automation** e.g., Decision based on thresholds/defined parameters.	Mandatory		
18	B2B Integration. **EDI Standards Support** (X12, EDIFACT, XML, JSON, File etc.). Support for EDI specific transports (HTTP/s, FTP/SFTP, AS2). Partner Onboarding and Management. B2B transaction security, insights and management.	Mandatory		
19	APIs cataloguing and auto discovery capability to enable reuse of existing APIs	Essential		
20	The platform should enable AI based **data transformation tooling**, allowing for automatic conversion and manipulation of data formats, structures, or content.	Essential		
21	Virtualization [to test your API early and often]	Essential		
22	The platform should support **Intelligent Document Processing** like compression, extraction.	Optional		
23	Seamless integration with **serverless computing platforms** covering both cloud and on-premise setup	Optional		

4. **API Governance-**

The framework and set of practices to ensure the APIs are complete, compliant, and consumable.

Table C-5 API Governance

S no	**Requirements**	**Requirement Type**	**Complied Flag (A/B/C/D/E)**	**OEM/ Product/ Module Name**

1	Unified API life cycle management: The platform should be able to manage the **end-to-end API lifecycle.**	Mandatory		
2	**Service level agreements**	Mandatory		
3	API design compliance (**OWASP and Open banking standards**)	Mandatory		
4	The platform uses **swagger** to design, build, and document the APIs	Mandatory		
5	API implementation and **policy adaption compliance**.	Mandatory		
6	The platform **provides API versioning capability via API Manager**, enabling easy management of different API versions	Mandatory		
7	The platform supports **JWT (JSON Web Token) and OpenID Connect** token validation	Mandatory		
8	The platform should provide **OOB (Out of the Box) Quality of Service (QoS) policies** such as service availability, performance, integration	Mandatory		
9	**Custom governance** rule sets	Essential		

5. API Observability-

The ability to understand the internal state of a system from the data it produces and the ability to explore that data in detail.

Table C-6 API Observability

S no	**Requirements**	**Requirement Type**	**Complied Flag (A/B/C/D/E)**	**OEM/ Product/ Module Name**
1	The platform should support logging based on severity & criticality of the events like **Debug, Warning, Info, Fatal, Exception** etc.	Mandatory		
2	The platform should have the capability to **masking the Audit log** as per security requirements.	Mandatory		
3	The platform should have the ability to **extract data for forensics**.	Mandatory		
4	**Meta-Data Support**	Mandatory		
5	End to end monitoring: The platform should have **End to end monitoring capability including observability** (resource availability, stability, and performance), **predictive analytics and**	Mandatory		

	proactive response along with operational workflow.			
6	The platform should provide **OOB (Out of the Box) dashboards** for monitoring of the API health	Mandatory		
7	The platform should be able to **generate reports** based on the collected data in the form of **dashboards, PDF, XLS** to be used for support, resilience, Monitoring.	Mandatory		
8	The platform should provide **traceability capabilities** to track the impact and history of corrective actions taken on the system	Mandatory		
9	The platform should cater to **customized monitoring requirements** like **connecting to ROC** for improved observability.	Mandatory		
10	The platform should support **automated notifications** during **request compatibility issues**, **API token failures**, high response time with direct connection to ITSM for ticket raising	Mandatory		
11	The platform should provide **real-time data analysis and visualization** for live tracking of performance	Mandatory		
12	The platform database should **collect machine data, part production data**, and quality data to enable effective business performance management	Mandatory		
13	The platform should provide **log management capabilities** to collect, store, and analyze log data generated by various components and systems	Mandatory		
14	The platform should support **log creation for detailed information** on behavior of applications and integrations	Mandatory		
15	**Custom analytics reports** and **AI-based anomaly detection** should be supported by the platform	Essential		
16	The platform should **automatically track and assign corrective actions** to appropriate personnel or teams	Essential		
17	The platform should provide **analytics capabilities** to monitor and analyze the usage, performance, and effectiveness of APIs	Essential		

18	The platform should support **single pane monitoring** of all internal and external APIs	Essential		
19	The platform should provide **visualization capabilities to depict the network topology** and connections between various components and systems	Optional		

6. API Monitoring-

The process of gathering, visualizing, and alerting on pre-defined metrics in order to ensure that an API is meeting specific expectations. Platform monitoring tools embedded within the platform to be directly connected to the bank's Dynatrace/ Heal and ROC setup. Services for determining performance of the EIS 2.0 platform, which includes monitoring tools and corresponding advanced analytics to pre-emptively fix issues.

Table C-7 API Monitoring

S no	**Requirements**	**Requirement Type**	**Complied Flag (A/B/C/D/E)**	**OEM/ Product/ Module Name**
1	The platform should provide **single pane of glass for applications, microservices, Monitoring and Analytics**.	Mandatory		
2	**Async API Monitoring**.	Mandatory		
3	The platform should provide **centralized monitoring for Integration** and API Management components	Mandatory		
4	The platform should provide **Alerts, Log Management, Reports, Health Check Monitoring, Business activity monitoring** via Custom Metrics, Application network visualization, API and integration analytics.	Mandatory		
5	The platform should have **capability to trace end to end customer interactions**.	Mandatory		
6	**Customized monitoring requirements** like connecting to ROC for improved observability.	Mandatory		
7	The platform should have **out of box dashboard for unified APIs**, orchestrated APIs, Common APIs, etc.	Mandatory		
8	Auto-Escalation.	Essential		
9	Auto-Ticketing.	Essential		
10	The platform should provide **Real-time data analytics.**	Essential		

11	The platform should provide **Business performance measurement** for banking services	Essential		
12	**Reuse & ROI Metrics**.	Optional		

7. API Commercialization-

The Bank can decide basis on the consumption of API's and responses from the platform.

Table C-8 API Commercialization

S no	Requirements	Requirement Type	Complied Flag (A/B/C/D/E)	OEM/ Product/ Module Name
1	The platform should be able to support charging models.	Mandatory		
2	The platform should provide support for multiple models of API commercialization	Optional		

8. API Publishing-

The process of making the APIs available to app developers for consumption.

Table C-9 API Publishing

S no	Requirements	Requirement Type	Complied Flag (A/B/C/D/E)	OEM/ Product/ Module Name
1	The platform should be able to download APIs as connectors for reuse.	Mandatory		
2	The platform should be able to discover and reuse existing assets (event driven APIs).	Mandatory		
3	Availability of reusable asset of API management for data mapping, transformation, orchestration and business logic flows	Mandatory		
4	Central asset repository to keep track of APIs and assets built on platform to manage API, examples, connectors	Essential		
5	The platform should enable Auto documentation of APIs with standardized documentation	Essential		
6	The platform should support auto generation of developer portal from API schemas and meta-data	Essential		

9. Messaging-

Application pushes a message into a queue by providing an asynchronous communications protocol. Queuing service to manage message queues, ensure reliable and asynchronous data exchange.

Table C-10 Messaging

S no	Requirements	Requirement Type	Complied Flag (A/B/C/D/E)	OEM/ Product/ Module Name
1	The platform should provide **Message broker and queueing pattern**. Advanced messaging capabilities, including routing, queuing for message storage and retrieval	Mandatory		
2	The platform should support **unicast and broadcast.**	Mandatory		
3	The platform should provide integration with external messaging platform: **Kafka, MQTT, JMS, MQ** and others, allowing for seamless integration and communication	Mandatory		
4	The platform should provide support for converting data from one format or protocol to another, such as **SOAP to REST, XML to JSON, JSON to XML, and XSL etc.**.	Mandatory		

10. Deployment-

The process of making the API callable by deploying on containerized based architecture.

Table C-11 Deployment

S no	Requirements	Requirement Type	Complied Flag (A/B/C/D/E)	OEM/ Product/ Module Name
1	All components like **API Gateway, ESB etc**. should be fully compatible and scalable in the Bank's **current Private cloud (ex: Meghdoot) infrastructure**.	Mandatory		
2	The platform should provide support for **geo-redundant deployment strategy.**	Mandatory		
3	The platform should provide support for **integrating with CI/CD pipeline** platforms like: **Jenkins, Maven, Azure etc. and other available CICD tools in the Bank.**	Mandatory		
4	The platform should provide support for **Maven, Ant**, etc.	Mandatory		
5	The platform should be **cloud native & cloud ready** and have the capability to be deployed on demand.	Mandatory		
6	**Managed cloud deployment**.	Mandatory		

7	Public/ private cloud deployment with no vendor lock-in.	Mandatory		
8	The platform should be **CNCF Compliant**: Cloud Native Computing Foundation (CNCF) compliant Kubernetes deployment - Same code to work in all environments.	Mandatory		
9	The platform should provide support for **blue/green deployment**, allowing users to create and manage two identical environments (blue and green)	Mandatory		
10	The platform should provide **configurable automatic back up & restoration mechanism.**	Essential		
11	The platform to have **inbuilt DevSecOps capability**.	Essential		
12	The platform should support **on premise deployment** and able to provide all features on premise and have **no linkages to models/algorithms in cloud.**	Essential		
13	The platform should provide capabilities to **override API response calls** in case of system downtimes or issues, and process data later as batches	Essential		
14	The platform should provide support for **infrastructure as code** (IAC)	Optional		

11. Scalability-

The ability of a system to handle an increasing amount of load while still delivering fast response times. Streaming capabilities to allow for efficient transfer of large amounts of data in real-time.

Table C-12 Scalability

S no	**Requirements**	**Requirement Type**	**Complied Flag (A/B/C/D/E)**	**OEM/ Product/ Module Name**
1	The platform should be capable of handling the **volume of the Bank** and to be the single API gateway for the Bank.	Mandatory		
2	The platform should support **Auto scale and self-heal and auto repair capabilities.**	Mandatory		
3	The platform should provide **Non-blocking I/O, Microservices with containerization Support**, Streaming capabilities, Parallel processing.	Mandatory		

4	The platform should have the capability to **configure tuning parameters for clustering and high availability.**	Mandatory		
5	The platform should be able to **handle TPS of more than 7000**.	Mandatory		
6	The platform should have support for **asynchronous mechanism enabled** for improved scalability and resilience.	Mandatory		
7	The platform should be capable of **rate limiting and throttling between different consumers**	Mandatory		
8	The platform should provide **horizontal scaling capability** to accommodate increased traffic and workload	Mandatory		
9	The platform should provide **streaming capabilities** to allow for efficient transfer of large amounts of data in real-time	Mandatory		

12. Latency-

The amount of time taken by the API to respond to a request.

Table C-13 Latency

S no	**Requirements**	**Requirement Type**	**Complied Flag (A/B/C/D/E)**	**OEM/ Product/ Module Name**
1	The platform should be able to provide **quick average turnaround time** of API delivery	Mandatory		
2	The platform API gateway should be able to support **more than 4 MB payload size**	Mandatory		
3	The platform should have the capability of **Payload compression**.	Mandatory		
4	The platform to have support for **Service Mesh capability** for high availability.	Mandatory		
5	The platform to have **Out of the box resiliency for network failures** and service communication by facilitating throttling and circuit breaker architectural patterns.	Mandatory		
6	The platform should support **Maximum Payload size**	Essential		
7	The platform should have capabilities of **Cache management**.	Essential		
8	The platform to have the **batch run capability**.	Essential		
9	Distribution of traffic across mesh. **Easily configurable API timeouts** based on API scenarios.	Essential		

13. Architecture-

API Architecture is a set of rules and practices that provide a framework for designing, developing, and delivering web services. API architecture defines how an application programming interface (API) interacts with the other components in its system.

Table C-14 Architecture

S no	Requirements	Requirement Type	Complied Flag (A/B/C/D/E)	OEM/ Product/ Module Name
1	The platform should have capability for **orchestration by configuration** i.e. multiple APIs from different applications with minimum efforts and timelines.	Mandatory		
2	Drag/ drop based orchestration	Mandatory		
3	Easy request response transformation	Mandatory		
4	The platform should have capability for **API choreography** - process where multiple subscribers react to a single event, using the data received for their own purposes	Mandatory		
5	The platform should support **API led microservices** and journey aggregations.	Mandatory		
6	The platform should have the capability of **event based triggering support mechanism** and support event driven architecture.	Mandatory		
7	The platform to support **Service Component Architecture** (SCA) - a set of specifications at describe a programming model for building applications and systems using a Service-Oriented Architecture (SOA)	Mandatory		
8	Availability of ESB within platform should **support legacy applications** and enable seamless integration with modern architectures	Mandatory		
9	ESB should serve as a **single-entry point for external systems** through an API gateway.	Mandatory		
10	ESB should support **orchestration and integration of loosely coupled components**, especially for legacy applications	Mandatory		
11	The platform should provide **complex event recognition**	Mandatory		

	capability, allowing the system to identify and respond to complex events.			
12	The platform should support **streaming of events**, enabling real-time processing and analysis of event data.	Mandatory		
13	The platform should provide **asynchronous API communication support**, allowing for non-blocking and event-driven interactions between components or services	Mandatory		
14	The platform should provide the capability to **compress payloads to save bandwidth** and reduce latency in some situations	Mandatory		
15	Service mesh architecture to provide a **dedicated infrastructure layer for managing service-to-service communication**, ensuring scalability, reliability, and observability	Mandatory		
16	The platform should support **API request queuing, retrieval and routing options** to be available to manage peak transaction workload	Mandatory		
17	The platform should support for **multi-clustered gateways and micro gateways** for customized entry points per use case	Mandatory		
18	The platform should enable **Master API to be bifurcated into multiple smaller APIs endpoints** for smooth functional changes and faster change deployments	Mandatory		
19	The platform should support **micro gateway** for accessing individual microservice through a separate gateway	Essential		
20	The platform should have a **clearly defined payload capacity at LB and WAF levels** for correct response capturing and smooth transaction flow	Essential		

14. Security-

Enforcement of bank-vetted security and authentication protocols for the hosted APIs to protect against unauthorized access or potential DDoS attacks.

Table C-15 Security

S no	Requirements	Requirement Type	Complied Flag (A/B/C/D/E)	OEM/ Product/ Module Name
1	The platform should provide **message level encryption** support to protect the confidentiality and integrity of data during transmission	Mandatory		
2	The platform should enable async **API Management and Security.**	Mandatory		
3	The platform should have a component on **Security Module** along with **enterprise level platform**, application and API security adoption.	Mandatory		
4	The platform should provide support for **multiple security protocols.**	Mandatory		
5	The platform should provide support for multiple encryption algorithms protocols like **AES 256, SHA, 256 etc.**	Mandatory		
6	The platform should support **OOTB policies** for **message threat protection**, **IP allow/blocklist** and header injection/removal.	Mandatory		
7	JWT and OIDC token validation.	Mandatory		
8	OOTB Quality of service policies.	Mandatory		
9	The platform should be able to support **hardware security module (HSM)**	Mandatory		
10	The platform's Compliance should be equivalent to payment systems including **PCI DSS by not storing card data on the platform**	Mandatory		
11	The platform should support **Tokenization, Nonrepudiation mechanism**s e.g. JWT, OAuth2	Mandatory		
12	The platform should provide the ability to handle **electronic signature verification** e.g., Digi-sign verification.	Mandatory		
13	The platform should support **field level encryption, basic authorization, fine grained authorization and identity management**.	Mandatory		
14	The platform should support all **access management** related requirements of the Bank.	Mandatory		
15	The platform should support **native feature richness** for authorization and	Mandatory		

	authentication: OAuth2, OpenID Connect, other protocols			
16	The platform should provide **secure configuration files**.	Mandatory		
17	The platform should provide **third party OIDC integration capability.**	Mandatory		
18	The platform should support **logging with meta data** and provide log extraction for analysis	Mandatory		
19	**Encryption or masking of API** objects or data points until consumed through code workflow within systems	Mandatory		
20	The platform should support **WAF, TLS v1.2, v1.3 etc.**	Mandatory		
21	WAF supervision for API endpoints to be domain based for preventing unauthorized or dummy transactions	Mandatory		
22	The platform should support **multiple encryption algorithms** protocols such as RSA, AES, hashing etc..	Mandatory		
23	The platform should support **SAML (Security Assertion Markup Language)** for secure single sign-on (SSO) and identity federation	Mandatory		
24	The platform should provide **Message level encryption, Field level encryption, Basic Auth**, SAML, Fine grained authorization, Identity management	Mandatory		
25	The platform should provide **identity management features** to manage user identities, including user provisioning, authentication, and authorization	Mandatory		
26	**API vulnerability detection capabilities** like injection, broken authentication, and insecure deserialization.	Mandatory		
27	Vulnerability detection for incidents such as **SQL injection**, **cross-site scripting** (XSS), and **XML external entity** (XXE) attacks	Mandatory		
28	**OOB (Out of the Box) support for mutual TLS (Transport layer security)**, for encryption and authentication of all communication between services	Mandatory		

29	The platform should enable API vulnerability detection capabilities like **injection, broken authentication, and insecure deserialization.**	Mandatory		
30	The platform should provide vulnerability detection for incidents such as **SQL injection, cross-site scripting (XSS), and XML external entity (XXE) attacks**	Mandatory		
31	The platform should provide a **real-time central configuration file** of API endpoints to manage API activeness and smooth service degradation	Essential		
32	API module and other systems should have relevant IP and port whitelisted for managing the API consumption and security	Essential		
33	The platform should provide VPN tunnel for providing a secure messaging channel for communication	Essential		

15. Third-Party Integrations-

Connectors to major third-party services to facilitate smooth interaction of APIs with external tools.

Table C-16 Third-Party Integrations

S no	**Requirements**	**Requirement Type**	**Complied Flag (A/B/C/D/E)**	**OEM/ Product/ Module Name**
1	Managing APIs deployed anywhere.	Mandatory		
2	**Third party identity provider integration** capability with audit trails.	Mandatory		
3	The platform should support **integration with third-party OpenID Connect (OIDC)** providers for user authentication	Mandatory		
4	The platform supports integration with **third party monitoring tools like Heal, Dynatrace** and other similar tools	Mandatory		
5	The platform should have **out of the box connectors** with easy integration with **third-party services such as Amazon S3, Jira** etc. to facilitate smooth interaction of APIs with external tools	Mandatory		
6	The platform should support **API Auto-cataloguing.**	Essential		
7	The platform should provide **API Auto discovery.**	Essential		

16. Compliance with Standards and Regulations-

Adhere to global compliance standards.

Table C-17 Compliance

S no	Requirements	Requirement Type	Complied Flag (A/B/C/D/E)	OEM/ Product/ Module Name
1	The platform should follow **Global Standards like Open Banking, BIAN standards, etc.**	Mandatory		
2	The platform should follow **Global Specifications like OpenAPI**	Mandatory		

17. Portability-

API portability is the ability to easily and flexibly move an API from one technology vendor/platform and/or cloud provider to another as part of a business transformation initiative.

Table C-18 Portability

S no	Requirements	Requirement Type	Complied Flag (A/B/C/D/E)	OEM/ Product/ Module Name
1	The platform should be able to support various **version control tools e.g. Jenkins**	Mandatory		
2	The platform to have ability to deploy on **containerized based architecture.**	Mandatory		
3	**Vendor and cloud portability** to reduce partner lock-ins for products	Mandatory		
4	Presence and maturity of platform APIs to enable **Infrastructure-as-Code (IaC)**	Mandatory		

Products / Components proposed in the BID

Table C-19 For products under Integrated Product Suite (Unlimited license)

S no	Component/ Software/ Tool's Name	OEM	Description

Table C-20 Other Products / Components

S no	Component/ Software/ Tool's Name	OEM	Unlimited License (Yes/ No)	Description

Table C-21 Bank's Products / Components proposed to be used

S no	Component/ Software/ Tool's Name	Usage proposed

We, hereby, certify that the above information furnished by us is complete and correct.

Name & Signature of authorised 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 1. Name 2. Designation 3. Address 4. Phone Number (Landline) 5. Mobile Number 6. Fax Number 7. Email Address	
9	Details for EMD Refund (applicable only if EMD is directly credited in designated account):- • Account No. • Name of account holder • Name of Bank • IFSC Code	

Name & Signature of authorised signatory

Seal of Company

Appendix-E

Scope of Work and Payment Schedule

E1. CONTEXT AND OBJECTIVES

Background:
State Bank of India is one of India's largest Bank with the network of over 24,000+ branches and 62,000+ ATMs spread across India. It is present in 32 countries across the globe and offers a wide range of products and services to both corporate and retail customers.
SBI has implemented Enterprise Integration Services (EIS) platform as a middleware to standardize integration among different channels and backend applications. EIS is extensively used by both upstream and downstream applications (Internal-176 and external-60). Critical channel applications are heavily dependent on this. The platform also has a few in-built orchestrated journeys, implemented at proprietary ESB layer.

Business rationale:
SBI intends to create technological resilience for its critical technology platforms. Presently Bank uses EIS as a critical middle layer application. EIS uses IBM technical stack (API Connect, Data power, ACE, IBM MQ etc.). Under this context, **SBI now invites the bidders to bid for building and installing Enterprise API Integration and Management Platform using alternate technology** other than the current EIS. This new platform will complement and supplement the existing EIS.

Objectives:
With the rising API consumption and dynamic Fintech requirements, bank has decided to have a strategic evolution in its API management, leading to the proposal for an additional API Integration platform *(aka Enterprise API Integration and Management Platform aka Enterprise Integration services Platform aka API Management Platform aka EIS 2.0*) that would complement and supplement the Bank's existing EIS with its strong orchestration capabilities and value-added features.
Below are the proposed objectives and expected benefits:

- **Enhance Service Resilience**: Alternate technology would help in significantly improving service resilience for both intra and inter-service. It would ensure robustness and reliability of the Bank's integration platforms. Alternate technology will also benefit in effective management of:
  - ✓ Internal Vs External
  - ✓ Public Vs Private
  - ✓ Retail Vs Corporate
- **Enterprise level Common Services:** Providing common services usable across various applications, streamline processes, improve efficiency and enhance overall user and developer experience.
- **Accelerated Time to Market:** Reduced integration timelines would give a competitive edge.

- **Dynamic Scaling and Self-Healing:** Dynamically scale resources to accommodate changing workloads. It would possess self-healing capabilities for automatic recovery of failed instances.
- **Advanced Technologies for High Availability:** 99.99% service availability through Service Mesh, Containers, Active-Active setup across sites and eliminate the need for manual intervention.
- **Orchestrate Services:** By orchestrating services for quicker delivery, the Bank aims to bolster Fintech engagement, drive innovation, and capitalize on monetization opportunities. The new platform will facilitate Fintech collaboration through a Journey Workflow Sandbox, allowing for seamless integration and experimentation.
- **Complement Existing EIS Platform:** EIS 2.0 is designed to complement the existing EIS platform, thus providing an additional layer of support and flexibility. It is expected to improve the overall efficiency and responsiveness of the Bank's services, meeting the evolving needs of customers and staying ahead in the competitive financial landscape.

E2. DESCRIPTION OF PRODUCT/SERVICES

E2.1 TO-BE ARCHITECTURE STRUCTURE

The development of EIS 2.0 involves integration of a new Enterprise API Integration and Management Platform with internal and external applications to complement the functionalities of the existing EIS 1.0 platform.

The bidder is expected to onboard the new Enterprise API Integration and Management Platform between the channels and the bank's core backend systems to orchestrate atomic API calls originating from the existing platform. At the same time, the platform is expected to directly establish connections with the various databases, core systems, and external systems and share some of the load of the existing platform.

A high-level view of the architecture can be found below:

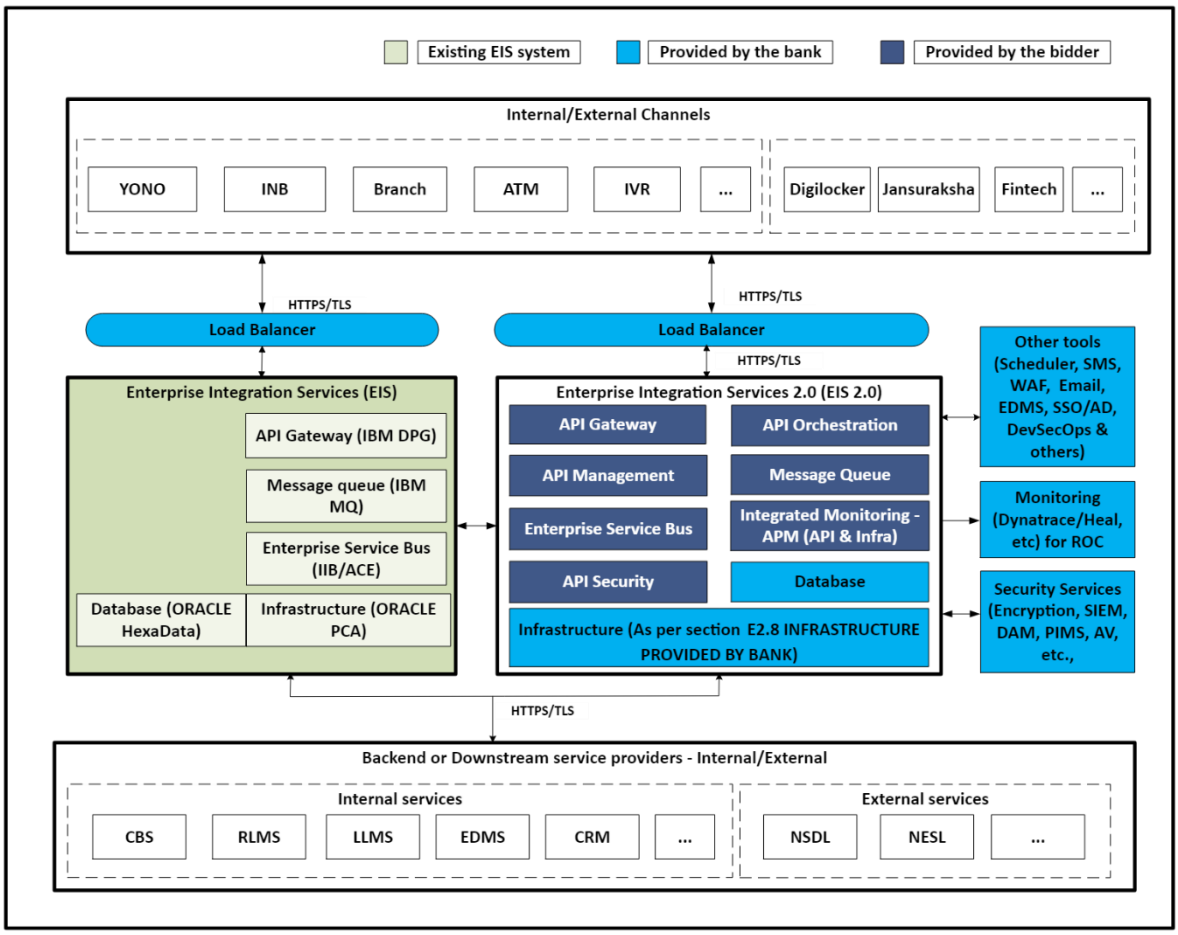

Fig E.1 Proposed Architecture

As part of the overall EIS 2.0 architecture, the bidder is expected to bring in multiple components as part of the end-to-end solution proposed by them. The bidder's architecture will be supported by the bank's existing systems by provisioning specific architectural components for the purpose of EIS 2.0.

Please note that the components shown in the figure are illustrative and may be modified based on the bank's requirement.

E2.2 EIS 2.0 - ENABLING PLATFORM FOR ENTERPRISE INTEGRATION

The bidder must ensure a scalable Platform (Integrated Product Suite) for the State Bank of India (SBI) that enables seamless integration across the bank's enterprise systems. The platform should support a unified, bank-wide integration strategy while providing a multi-tenant setup that allows various departments and applications to independently leverage, expose, and consume services. Additionally, the platform must facilitate controlled cross-tenant interactions to enhance collaboration and operational efficiency.

Platform Architecture and Design

The selected bidder is required to deliver the following scope of work as part of this project:

- **Develop a Multi-Tenant Architecture**: Design and implement a robust multi-tenant architecture that ensures data and resource isolation while allowing shared infrastructure utilization
- **Implement Microservices-Based Architecture**: Leverage a Microservices architecture to ensure modularity, scalability, and independent service deployment for various banking functions
- **Adopt Event-Driven Integration**: Implement event-driven architecture to enable real-time data exchange and processing across SBI's systems
- **Integrate Service Mesh**: Utilize service mesh technology to manage inter-service communications, providing capabilities like observability, traffic management, and security for Microservices within the platform

Tenant Management

- **Establish Tenant Isolation Protocols**: Ensure strict isolation of data, configurations, and resources between different tenants (departments, applications) within the platform
- **Enable Tenant-Specific Configurations**: Provide customizable configurations for each tenant, including resource allocation, service-level agreements (SLAs), and security settings
- **Facilitate Controlled Cross-Tenant Access**: Develop and implement policies for secure and controlled cross-tenant interactions, enabling collaboration between departments while maintaining compliance and security

Service Exposure and Consumption

- **API Management Framework**: Deploy a comprehensive API management framework so that various tenant can securely expose, manage, and monitor APIs. This should include features such as versioning, authentication, authorization, and analytics
- **Centralized Service Catalog**: Develop a centralized service catalog for the discoverability of all exposed services, providing metadata, usage guidelines, and documentation
- **Service Discovery Mechanism**: Implement a dynamic service discovery mechanism to manage service endpoints and ensure seamless communication between services

Integration Capabilities

- **Provision Pre-Built Connectors**: Provide a library of pre-built/ standardized connectors, as applicable, for various internal applications such as CBS, RLMS etc., and external applications such as CRM, ERP etc. and other enterprise applications available with the Bank to facilitate rapid integration
- **Data Transformation Tools**: Offer robust tools for data transformation and mapping, supporting diverse data formats and ensuring smooth data exchange across different systems

- **Orchestration and Workflow Automation**: Implement capabilities for orchestrating complex integration workflows, including support for long-running transactions and compensation mechanisms

Security and Compliance

- **Identity and Access Management (IAM)**: Integrate with SBI's IAM systems, single sign-on (SSO), multi-factor authentication (MFA), Privilege Identity Management System (PIMS) and centralized user management etc.
- **Data Encryption and Protection**: Ensure data is encrypted at rest, in transit and in motion. Implement secure key management practices, data masking and tokenization for sensitive information.
- **Compliance and Audit Trail**: Implement comprehensive compliance management and audit trail features to meet internal and external regulatory requirements and facilitate reporting and monitoring.

Detailed Security requirements are mentioned in Section E12. (Of this Appendix).

Monitoring and Performance Management

- **Centralized Monitoring Platform**: Establish a centralized monitoring and logging platform to track the performance, health, and security of all services and integrations with the central monitoring systems as per the requirement of Bank.
- **Analytics and Insights**: Provide tools for real-time and historical analytics, enabling detailed insights into service usage, performance trends, and anomaly detection
- **Self-Healing and Scalability**: Implement auto-scaling and self-healing capabilities to ensure high availability and resilience of the platform

Cross-Tenant Leveraging

- **Enable Inter-Tenant Data Exchange**: Develop secure and controlled mechanisms for inter-tenant data exchange to support shared business processes and collaborative reporting
- **Shared Service Models**: Create shared service models that can be accessed across tenants with defined ownership, access controls, and usage policies
- **Policy Enforcement**: Implement policies at the platform level to govern data residency, privacy, and usage constraints for cross-tenant interactions

Developer and Operations Support

- **Developer Portal**: Establish a developer portal with access to APIs, documentation, and sandbox environments, enabling developers to test and integrate services efficiently
- **DevSecOps Integration**: Support integration with continuous integration/continuous deployment (CI/CD) pipelines, automated testing, and deployment workflows

- **Multi-Language Support**: Provide support for multiple programming languages and frameworks to accommodate diverse development requirements

Scalability and Flexibility

- **Cloud-Native Infrastructure**: Utilize cloud-native technologies (e.g., Kubernetes, Docker) for scalable and flexible infrastructure management
- **Hybrid Deployment Models**: Support hybrid cloud and on-premises deployment models, allowing seamless integration and scaling across different environments

Governance and Management

- **Service Governance Framework**: Develop and implement a governance framework to manage the lifecycle of services, including design, deployment, versioning, and deprecation
- **Usage and Billing Management**: Implement mechanisms for tracking usage and generating billing or chargeback reports for resource utilization by different tenants.
- **Change Management Processes**: Establish change management processes to handle updates, migrations, and service modifications with no disruption

E2.3 DETAIL ON THE TECHNOLOGY PLATFORM COMPONENTS

Proposed solution should contain components including:

API Gateway: The proposed Integrated Product Suite, should include an API gateway to manage incoming requests, **orchestrate** and route them based on key factors (request path, headers, query parameters, etc) for efficient **distribution of traffic** and ensures proper **load balancing** among target endpoints.

API Management: The API life cycle of **designing, developing, testing, securing, monitoring, and analyzing** APIs. Also, include a **developer portal** where newly published APIs can be distributed along with their **documentation, publishing and discovery of APIs**.

Enterprise Service Bus (ESB): An architectural pattern by which a centralized software component performs **integrations** between applications.

Message Queuing Service: For **asynchronous messaging**, the message queues store messages that one applications create for other applications to use in the same order they are transmitted until the consuming application can process them.

Security: Enforcement of bank-vetted security, **authorization** and **authentication** protocols for the hosted APIs to protect against unauthorized access or potential attacks.

Integrated Product Monitoring: Process of collecting data for system's health check and generate alerts during failure. Also, to understand the system's internal state by analyzing the data (logs, metrics, traces, etc.,).

Commercialization Engine: The Bank can decide to charge the user basis the consumption of API's and responses from the platform.

Deployment with Containers: To provide a secure, reliable, and lightweight runtime environment for the portable deployment into Bank's private cloud environment (ex: **Meghdoot**).

Cache management: APIs, caching is used to improve the response time of requests by storing the results of frequently-used requests in a cache.

Connectors: Pre-built software packages to interact with third party external applications or data sources.

Any other tools / components required to set up and operationalization of EIS 2.0 platform as per scope of the RFP.

It is preferable that the bidder should bid with minimum number of 3rd party OEMs/ components.

E2.4 TECHNICAL REQUIREMENTS

Details of the Technical Capabilities and Components required for Enterprise API Integration and Management Platform are mentioned in **Appendix-C.**

The bidder has to fill and submit this format duly signed by the authorized signatory.

E2.4.1 HIGH AVAILABILITY AND MONITORING REQUIREMENTS

Active-Active architecture

The bidder has to ensure proper implementation to meet resiliency architecture for data where workloads are distributed across two or more nodes in a cluster to keep the data safe and available in the event of an unexpected component failure.

Bidder is also expected to maintain high availability of Enterprise API Integration and Management Platform and corresponding services across data centers and availability zones and load balancing across availability zones

Circuit Breaker

Bidder has to enable circuit breaker architecture as part of the solution. Circuit breaker is a design pattern used in software development to detect failures and encapsulate the logic for preventing a failure from constantly recurring. It is used during maintenance, temporary external system failure or unexpected system difficulties.

High Availability

The bidder has to ensure high availability of the Enterprise API Integration and Management Platform and corresponding services by ensuring implementation of disaster recovery approach with RTO/RPO alignment with corresponding metrics, employing a multi-

region/multi-cluster approach and parallel implementation of incoming platform with the existing EIS 1.0 and related services

Observability and Monitoring Requirements

The BIDDER has to ensure comprehensive monitoring of key metrics for EIS 2.0, including transaction counts, load times, service response, and system availability. A detailed list of these metrics will be collaboratively created by the BIDDER and the Bank. All defined metrics should be actively monitored:

- Application Monitoring: The BIDDER has to provide enterprise-level Application Performance Monitoring (APM) and synthetic monitoring tools for real-time, 24x7x365 monitoring of infrastructure and applications. This includes dashboarding, reporting, and alerting stakeholders, integration into the Bank's command center etc.
- Infrastructure Monitoring: The BIDDER has to implement tools and ensure comprehensive infrastructure monitoring, covering servers, databases, and other backend components within the EIS 2.0 environment.
- End-to-End Observability: The BIDDER has to deliver tools and expertise for enhanced observability across the EIS 2.0 ecosystem, providing monitoring dashboards to facilitate efficient system maintenance.

Disaster Recovery

The three main sites should be physically separated and located in the same city, in compliance with all near DR policies. The three sites should be maintained with High Availability (Active-Active deployment at both sites) The DR switchover must be completed in a maximum of 15 minutes. The replication between the Primary and Secondary sites should be possible in both directions. All components (hardware and software) at all sites should be an exact replica of the primary site.

E2.5 FUNCTIONAL REQUIREMENTS FOR EIS 2.0

The Enterprise API Integration and Management Platform will ingest APIs exposed by the bank's existing EIS and other connections (core systems, external systems and databases etc.) and offer a bouquet of services to all channels consuming the data (YONO, RINB, CINB etc.). Some of the service buckets are listed below, with non-exhaustive lists of APIs included with them. Bank can advise additional APIs to be developed and published during the contract period as per requirement of the bank.

Please refer "Table E-6" for estimated APIs to be developed, orchestrated and published.

ILLUSTRATIVE LIST OF SERVICES TO BE DEPLOYED AS PART OF EIS 2.0

1. **Retail:** The Enterprise API Integration and Management Platform is expected to host services related retail banking functionalities to the bank customers. This list is indicative and non-exhaustive. Please note that the number of services per milestone might be modified by the bank based on business requirements.

Table E-1 Retail Services

Service Bucket	Name of Service	Description
	CIF Enquiry	Validate existing bank user using their CIF details for login authorization

Registration and Login	Customer Enquiry	Fetch additional customer details to populate landing page for user
	Aadhaar Fetch and Validation	Fetch Aadhaar details from the Aadhaar Vault to validate KYC for customer
	Set Profile Password	Set profile password to authorize payment transactions, account configuration changes and registration for add-on services
Savings Account	CIF Creation	Create Customer Identification File for New-To-Bank user using KYC details and other personal details
	Account Opening	Creation of new bank accounts (savings, FD etc.) with necessary customer details and redundancy checks
	Aadhaar-based KYC	Securely store Aadhaar details to ensure compliance and fetch KYC information on need basis for opening savings account
	Video KYC	Automated video KYC journeys for customer verification
	DigiLocker	Integrate with Digilocker for secure storage, retrieval and validation of digital documents such as marksheet, ration card, registration certificate
	Account Statements	Fetch account statement for a savings account for internet banking or YONO
	Create Nominee	Enlist nominee with complete personal details and KYC for savings account
	Update Nominee	Modify nominee or personal details for savings account
Loans and Deposits	Loan Account Creation	Create loan account post KYC and assessment of previous financial health and credit scores
	Deposit Creation	Create loan account post KYC and assessment of previous financial health and credit scores
	Repayment Scheduling	Create repayment schedule post calculation of EMI value and repayment duration
	SI Management	Create and manage Standing Instructions for streamlining repayments for loans
	Rate of Interest Calculator	Calculate rate of interest based on customer history and other offers such as student discounts etc.
	NPA Evaluation	Evaluate loan's status as an NPA based on parameters such as repayment history, customer CIBIL scores etc.
	CIBIL Score Validation	Fetch credit score from CIBIL to be utilized in creditworthiness assessment
Fund Transfer	Beneficiary Management	Addition and modification of beneficiaries for making payments using direct transfer methods
	NEFT Fund Transfer	Direct bank-to-bank transfer via SFMS rail with batch processing for transactions
	IMPS Fund Transfer	Direct bank-to-bank transfer on a real-time settlement process using NPCI IMPS rail

	RTGS Fund Transfer	Direct bank-to-bank transfer on a real-time settlement process for high-value transactions
	Create Limit	Create account-specific limits for different payment types (card payments, international payments etc.)
	Update Limit	Update account-specific limits on instant basis using mobile app or internet banking portal
Debit Cards	Customer Profiling	Fetch debit card spend data and customer profile data to suggest more banking products
	Apply for Debit Card	Initiate credit card application post savings account creation or on need basis
	PIN Management	Modify PIN used for ATM or POS transactions with the debit card
Bill Payments	Biller Details	Fetch details of biller for maintaining dashboards for biller portal
	Bill Payment	Initiate bill payment order to be processed using UniPay portal
	Bill Validation	Validation of bill generated by online and offline billers hosted on BBPS and non-BBPS merchants
	Raise Billing Complaint	Raise complaint for payment failures or other issues on UniPay
	Track Complaint Status	Track status of complaints filed as part of UniPay payments
	Create SI	Create a Standing Instruction for recurring payment requests
	Update SI	Update Standing Instruction for recurring payment requests
	MOPS Payment	Create payment request for SBMOPS (ePayLite) for credit/debit cards for UniPay portal
	MOPS Refund	Generate refund request for SBMOPS (ePayLite) for credit/debit card payments for UniPay
	UPI Payment	Create payment request for SBMOPS (ePayLite) for UPI payments for UniPay portal
	UPI Refund	Generate refund request for SBMOPS (ePayLite) for UPI payments for UniPay portal
UPI Payments	PSP Connection	Establish connection with linked PSPs (PayTM, WhatsApp, BHIMPay) to receive UPI transactions with SBI VPA
	VPA Creation	Create VPA for SBI account holder or user of one of the linked PSPs
	OTP-based Validation for Mobile Number	Validate customer mobile number account linkage using OTP
	Collection Notification	Receive notification of payment collection request via UPI
	Transaction Status	Track status of UPI transaction

	Mandate Management	Creation and execution of UPI Mandates for recurring subscription payments
	QR Code Creation	Create QR code corresponding to individual VPA address
	QR Code Validation	Resolve QR code detected by app into targeted VPA address
Credit Cards	Creditworthiness Assessment	Fetch CIBIL data, customer profile and banking history to evaluate repayment capability
	Alerts and Notification	Initiate alerts for credit card bill payment due date, transactions, password change, PIN change etc.
	Apply for Credit Card	Initiate credit card application post creditworthiness assessment, CIF validation and dedupe checks
	Offers and Discounts	Provide list of offers and discounts on third-party applications available on customer's existing credit card
Add-On Services	Reward Management	Earning and redemption of reward points earned as a result of account transactions
	ITR e-Filing Request	Create request for e-Filing of Income Tax Return by establish linking to ITR portal
	Wearable Management	Establish YONO pay on wearable devices such as Titan Pay Watch
	Gold Loan Account Creation	Create Gold Loan account post KYC validation, dedupe checks and offline validation of gold assets

2. **Corporate:** The Enterprise API Integration and Management Platform is expected to enable a host of corporate banking functionalities via multiple orchestrated APIs. This list is purely Commercial and non-exhaustive and will be finalized as per the detailed assessment.

Table E-2 Corporate Services

Service Bucket	Name of Service	Description
Onboarding	Document Upload	Upload documents such as company PAN card, incorporation certificate and GST certificate for onboarding corporate customer
	Account Creation	Create corporate banking account based on product type such as Saral, Vyapaar, Vistaar etc.
	CKYC Validation	Validate corporate banking customer KYC data
	AML/CFT Verification	Perform AML/CFT validations on new corporate banking customer before account creation
	GST Validation	Validate GST certificate of corporate banking customers prior to account creation
User management	Create User Profiles	Create user profile for corporate banking account usage with setting necessary roles and corresponding permissions

and administration	Manage User Profile	Modify role details and scope of permissions and access provided to the specific role
	Reactivate Blocked Account	Reactivate blocked/dormant user profile based on user request with pre-set configurations
	Audit User activity	Audit corporate banking customer and specific user activity to detect fraudulent or suspicious transactions
User experience	Digital signature	Fetch digital signature certificate from certification authority to be used for banking transactions
	Notification Creation	Create notification from account activity to be sent to customer devices
	Notification Deployment	Deploy notification as an alert to respective customer devices
	Non-transaction status request	Fetch status of requests on account configuration or complaints filed
	Single Sign-On (SSO) Authentication	Authenticate user profile using Single Sign-on authentication for access to specific user permissions
Virtual accounts	Create static virtual account number	Create static virtual account for corporate banking customers for handling series of recurring payments for one purpose or from one destination
	Create dynamic virtual account number	Create dynamic virtual account for corporate banking customers for temporarily handling one-off payments
	Create limit for existing virtual account number	Set transaction frequency and amount limit, along with user access for existing virtual account numbers
	Dashboard across virtual accounts	Fetch data from CBS and other systems to create dashboards for individual virtual accounts
	Update virtual account hierarchy	Modify hierarchy of virtual account in terms of which gets privileged access over others
Payments	Fetch FX Information	Fetch exchange rates for the purpose of international transactions in corporate banking
	Customize client rates	Modify deal rates offered to customer based on banking history, size of customer, transaction ticket size etc.

	Instant Payment (SARIE)	Initiate payments to Saudi Arabia-based customers via the SARIE payment system owned by Saudi Central Bank
	SWIFT GPI Payments	Initiate payments on the SWIFT GPI rail for international customers/partners
	Recurring payment automation (salary payments)	Create recurring payment mandate for salary disbursement function of corporate banking customers
	Non STP File / Transaction Approvals	Request non STP File / Transaction Approvals (for transactions initiated through B2B / SWIFT)
	Automated invoicing	Enable automated invoicing including generation of electronic credit invoice, collection files etc. and capturing information for reconciliation
	Reconciliation	Initiate auto reconciliation of payments/receivables against invoices/bills generated
	Upload Mandate	Upload payment mandate for handling large-volume recurring payments
Dividend payments	Onboarding dividend payment client	Onboard large-scale corporate banking customers for purpose for disbursing dividend payments
	Dividend accounts reconciliation	Reconciliation of all dividend accounts for a particular corporate banking customer
	Dividend processing (SAIB Account / SARIE / SWIFT)	Process dividend payments across multiple payment rails such as SWIFT, SARIE and SAIB (Saudi Arabia)
Liquidity Management	Set sweep trigger	Set maximum and minimum limits for when the fund transfer will actually take place from the account
	Set sweep duration	Set time limits for sweep account fund transfer
	Set sweep frequency	Set frequency of sweep transfers (Weekly, biweekly, monthly, quarterly etc.)
	Link accounts for pool creation	Link accounts into hierarchical structures of individual groups to create a multi-level cash pool
	Master account management	Maintain master account within multi-entity pool to which sub accounts can be linked

POS/ eCommerce Management	Generate POS Terminal Report	Generate report for PoS terminal transactions, reconciliation and dashboards
	Request New POS Terminal	Create new request for issuing a new PoS terminal for merchants post merchant KYC and onboarding
	Raise Request for POS Change	Raise request for changing PoS terminal in case of product defect or end-of-life for the machine
Trade Finance	Initiate Sanction Screening	Initiate sanction screening on incoming transaction to validate beneficiary/remitter details against sanctions of the source and destination country
	Initiate AML/CFT verification	Initiate Anti-Money Laundering/Countering the Finance of Terrorism checks against customer profile while account opening process
	Generate trade finance limit utilization report	Generate report for highlighting the extent of trade finance limit utilization and remaining scope
Guarantees	Create Bank Guarantee (Bid Bond/Retention Money/Buyers Credit/Mobilization Advance Guarantee)	Create bank guarantee of a particular type post completion of application mentioning details about beneficiary, amount, validity period etc.
	Initiate Outward Remittance	Initiate Outward Remittance
	Upload existing Bank Guarantee	Upload existing bank guarantee document/details to update on the portal/app
	Bulk Bank Guarantee closure	Initiate closure of large set of bank guarantees via bulk API call
	Initiate Bank Guarantee closure	Initiate closure of a particular bank guarantee post completion of its payment terms
Letter of Credit	Create Letter of Credit (merchandise/services/cash backed/capital goods, Revolving, Insurance etc.)	Create letter of credit of multiple types (merchandise/services/cash backed/capital goods, Revolving, Insurance etc.) with basic details

	Fetch notional exchange rate	Fetch appropriate notional / standardized exchange rate to convert letter of credit amount to base currency for issuance and amendment
	Validate beneficiary	Validate beneficiary for letter of credit utilizing banking history, KYC details and AML/CFT validations
	Generate SWIFT/SFMS message	Generate all types of Swift/SFMS messages pertaining to letter of credit issuance, amendment and bill acceptance
	Create bill	Capture bill details including details of goods, shipment details, transportation details etc
Supply Chain Finance	Capture Program Code details	Capture details in the program master for individual Program Code for each arrangement, commissions, dealers and suppliers
	Capture dealer details	Capture details of dealer from Program Code such as transaction limits, funds disbursal details
	Capture supplier details	Capture details of supplier from Program Code such as transaction limits, funds disbursal details
	Create pricing structure	Create multi-tiered pricing structure (e.g., by amount, period, percentage or flat charge, interest based with daily accrual), with minimum and maximum amount
	Create transaction split	Create a split of transaction charges between the parties – the buyer, seller or any other party
	Calculate deal-level interest	Calculate rate of interest on an individual deal-level by incorporating parameters related to buyer and seller details, ticket size etc.
	Pay advance or arrear-based interest	Make advanced or arrear-based interest payments on prior transactions or recurring payments
	Report Generation	Generate reports related to overall transaction data, or data specific to Program Code, individual dealer or supplier or time series based
	Calculate penalty interest rate	Calculate the interest rate on penalty
	Upload invoice file	Upload invoice file to capture details such as total amount, buyer and supplier details, list of goods etc.
	Upload bills and receipts	Bulk upload of bills, receipts and purchase orders to capture accumulated data across multiple receipts
	Validate invoice	Validate invoice for fraud, GST number, customer details etc. for further processing
	Set disbursement schedule	Set schedule for recurring disbursement of payments to suppliers for constant flow of money

	Process disbursement	Process actual disbursement on scheduled day of payment for actual credit to suppliers
Alerts	Insufficient Funds Alert	Raise alert or notification for insufficient funds in account
	Transaction Failure Alert	Raise alert or notification for a B2B transaction failure
	Scheduled Payment Alert	Raise alert or notification for a scheduled payment failure owing to insufficient funds, authorization failure or technical failure
Complaints	Raise Complaint	Raise complaint via Corporate INB portal or YONO Business app
	Check Complaint Status	Track complaint status for Corporate Business transactions
	WhatsApp Integration for Complaints	Establish WhatsApp connection to track and raise complaints directly
Dashboard	Fetch data from CBS	Fetch corporate banking account data and transaction data from CBS for customer dashboard
	Fetch data from Platform Monitoring	Fetch platform uptime data for monitoring and observability purposes
	Fetch customer data	Fetch customer configuration and profile data for customer analytics
Reports	Statement Analyzer	Analyze account statement for large corporate banking user for dashboarding and customer profiling
	Report Scheduling	Create schedules for generating reports of corporate banking account usage and transaction data
	PDF/XLS Report Generation	Convert report data generated into PDF or XLS format for user readability

3. Others: The Enterprise API Integration and Management Platform must also enable value-added services such as Wealth Management, Insurance, Agriculture-related benefits to provide a holistic experience to customers through end-user channels. This list is purely indicative and non-exhaustive and will be finalized as per the detailed assessment.

Table E-3 Other Services

Service Bucket	**Name of Service**	**Description**
Consent management	Capture consent	Capturing of the consent of the user
	Modify consent	Modifying the consent already captured for the user
	Query Consent	Inquire the consent status

	Delete consent	Deletion of the consent captured
Wealth	Validate PAN details	Validate PAN details using NSDL servers
	Validate KYC	
	Create Demat Account	Create demat account post customer KYC validation and PAN validation
	Upload Demat details from external platform	Fetch demat account created from external platform to display on YONO app
	Create Mutual Fund	Create Mutual fund account post customer information verification and confirmation of product offering chosen
	Set mandate	Set mandate for recurring payments for mutual funds with Monthly/quarterly/annual payments
	Update mandate details	Update mandate amount, frequency in case of investment policy change
	Create NPS Account	Create account for National Pension Scheme for individuals opting for the scheme
	Create PPF Account	Create account for National Pension Scheme for individuals opting for the scheme
	Fetch NPS Balance	Fetch NPS account balance to be displayed on portal/app
	Fetch PPF Balance	Fetch PPF account balance to be displayed on portal/app
Insurance	Create Insurance Application	Create insurance application post KYC, calculation of premium and finalization of policy type
	Fetch Insurance Application	Fetch incomplete application saved in bank system for completion of on-boarding journey
	Retrieve Quote	Retrieve premium quote provided based on customer data and other personal information
	Link Insurance Policy	Link policy purchased via an external third-party provider into the YONO app for ease of use
	Renew Insurance	Renew insurance policy with updated premium calculated using updated customer data
	Fetch Insurance Status	Fetch status of insurance in terms of whether it is active, premiums are paid on time etc.
	Update KYC	Update KYC details in case of major customer data change such as address change etc.
	Create Nominee	Create nominee for insurance benefits post insurance application confirmation
	Update Nominee	Update nominee details or modify nominee during insurance term

Others	NCMC Card Management	Create and top-up National Common Mobility Card for travel across public transport modes
	Create Kisan Credit Card Application	Create Kisan Credit Card application post customer KYC, dedupe checks and background check
	Fetch Agri Marketplace Data	Fetch data from multiple Agri marketplaces such as AGRIBEGRI, BigHaat, Kisan eStore etc.
	YONO Coins Management	Track usage and earning of YONO coins earned from frequent usage of YONO app

E2.6 NON-FUNCTIONAL REQUIREMENTS

The Non-Functional Requirements for EIS 2.0 platform:

Table E-4 Non-Functional Requirements

#	Objectives	Description
NFR 5.1	BCP	The proposed platform should provide an overall uptime of 99.99%. The Bidder has to provide complete document on Business Continuity plan (BCP) and Disaster Recovery Plan (DRP) for the proposed solution.
NFR 5.2	Redundancy	Active Passive Redundancy (rack and server level failure redundancy) and a high availability architecture
NFR 5.3	Performance	EIS 2.0 platform components shall operate with a maximum latency of 20 ms or less measured from an end-user's perspective when triggering and producing the output. (it should provide caching technology for high-performance requirements).
NFR 5.4	DR Routing	EIS 2.0 platform components shall provide the capability for routing based on criteria but not limited to content based, rule based, policy based the service request to the appropriate service providers
NFR 5.5	Failure Tolerance	Solution should be installed in multiple Data Centers.
NFR 5.6	Failure Tolerance	Solution should meet RTO - RPO and Availability requirement as per bank's policy/ requirement. Bidder should prove how solution can meet this requirement. Non-Disaster: - RPO: 0 mins -RTO: 5 mins Disaster: - RPO: 0 mins-
NFR 5.7	Availability	Load balanced across machines and utilization of active-active application configurations to avoid single failure point
NFR 5.8	Availability	Platform to be deployed in all the Data Centers of the Bank
NFR 5.9	Availability	Solution should be possible to run on heterogeneous multi-vendor hardware
NFR 5.10	Security	The application must adhere to LAN, Domain Controllers, firewalls and End Point security as managed by the Bank.

NFR 5.11	Security	API Manager must support role-based authorization (OAUTH with JWT token) and payload encryption (HSM/Public key)
NFR 5.12	Deployment	Bidder to provide the deployment Diagram of the solution.
NFR 5.13	Deployment	Bidder to provide the SOPs required for deployment of the solution.
NFR 5.14	Manageability	Solution should be able to easily debugging and have ability of logging of all components.
NFR 5.15	Resiliency Requirement	Non-Disaster: - RPO: 0 mins 99.99% of PR site data recovery -RTO: As per the prevailing Bank's BCM policy Disaster: - RPO: 0 mins-
NFR 5.16	Usability	Solution should have simple user interface and UI-UX.
NFR 5.17	Usability	Solution to have cross Browser support.
NFR 5.18	Back UP and archiving	Bidder will be responsible for both online and offline Backup up of Application and Database as per the requirement and policy of the Bank.
NFR 5.19	Activity Log management	Platform to have complete logging of all activities.
NFR 5.20	Activity Log management	Platform to have log aggregation agent.
NFR 5.21	Activity Log management	Platform to have inbuilt diagnostics and support feature.
NFR 5.22	Activity Log management	Platform to provide performance Report as required.
NFR 5.23	Activity Log management	Platform to provide Log retention as per the Bank's policy.
NFR 5.24	Auto Scalability	ESB shall provide horizontal and vertical scaling capability. Scale up and out as business needs grow.

E2.7 OTHER REQUIREMENTS

Below items are part of the scope but not limited to: -

Development:

i. API Mock Services for Interfaces
ii. DevOps Adoption
iii. Optimization of ESB flows across environments
iv. Development for New Protocols like DLT
v. Exposing APIs for open banking initiatives for Sandbox environment
vi. Revamp of EIS architecture as to utilise PaaS offerings available in Bank

Application Support:

i. Open Banking Support
ii. Business Dashboards creation and maintenance on OBIEE
iii. Problem/incident/fault/error Management - Identification to Closure
iv. Manage 300 Calls/score tickets per day

Infrastructure Support:

i. Support
   a. VMWare, TFS, APM tools like Dynatrace/ Heal, Load Balancer
ii. Upgrade & Migration
   a. Database like Oracle 19c, Oracle PCA etc.
iii. Configuration Management & Deployment support
iv. Adoption
   a. Bank's Private Cloud (ex: Meghdoot) PaaS
   b. DR Automation
   c. DevOps, Open API 3.0
   d. Developer Portal Sandbox environment
v. Storage & Archival

System Testing

i. NFR Testing - Periodic Load testing and assessment of EIS 2.0 performance
ii. Regression Automation with 95% test coverage

Project Management/Governance Control/Architecture

- Project Management
  i. Incident Management, Change Management
  ii. Development Delivery Planning
  iii. Monthly Progress and Health Report
- Governance & Control
- Architecture
  i. Open Banking Sandbox Initiative
  ii. Circuit Breaker Patterns and Throttling
  iii. MQ based Asynchronous Queue Based Processing
  iv. New Protocol introduction for downstream systems like DLT/Blockchain
  v. Scripting automation & incident ticketing automation
  vi. Platform features like DevOps, Containerisation, Open API 3.0
  vii. Service segregation
  viii. Workflow/Orchestration review and implementation on the platform

Production Support Activities:

- **Application monitoring -** This shall involve uptime monitoring of the EIS 2.0 APIs and applications.
  i. Monitor application uptime.
  ii. Monitor APIs/applications/interfaces that EIS 2.0 provides to external systems
  iii. Application monitoring tools to be used meticulously
  iv. Routine health check of the applications as per the checklist and methodology identified
  v. Be the primary point of contact for all incidents/issues in APIs and Applications reported via phone call, email, in person etc.
  vi. Monitoring of in-scope applications to external systems and a suitable report to be submitted to all application owners on all incidents and performance monitoring.

vii. RCA to be submitted for all incidents which are not routine in nature, workaround to be documented before execution and the signed RCA document to be submitted in the Bank's provided format by bidder representatives.
viii. Analyze the issues that do not require code changes
ix. Resolving queries and issues raised over emails and calls.
x. Resolve application issues that do not require code changes and are related to application deployment/environment only.
xi. For complex issues or issues requiring code changes, the points of contact for this team would be as per the agreed definition.

- **Monitoring and Support for scheduled Operations** - This involves daily monitoring of the jobs that runs on the production servers.
  This includes
  a) Monitoring, reporting of the Linux/Windows batch jobs including Shell, bash, PowerShell Script failure wherever appropriate. This list is not exhaustive and may include as per the logging and monitoring SOP of the bank revised from time to time.
  b) Support for execution of Archival jobs, maintaining log files, maintaining data files, mocks for period runs etc. This may also involve following housekeeping activities:
  c) Regular purging of old log files and data files.
  d) Regular purging of user specified files as agreed upon.
  e) Purging of relevant files.
  f) Extracting data/logs as required.
  g) Maintain an Issue Register/Issue Library for future reference.
  h) Production Issue Resolution
  i) Any other housekeeping activity as identified by bank or EIS 2.0 department

- **Status Reporting -** This involves preparing operations status report on Daily, Weekly and Monthly basis. This also involves below activities as per Bank's logging and monitoring policies including
  a) Preparation, submission, and review of SOP for the defined activities.
  b) API and Channel usage repository maintenance
  c) Providing requested reports including not limited to health performance of EIS 2.0 ecosystem, best practices implementation, recommendations implementation.

- **Support to channels and Operations -** This involves attending to the IT requests, incident as per the incident management policy, calls, mails, and queries on 24x7x365 basis from various channels/departments like YONO, RLMS, FIGS, ATM, UPI, PSG, CMP, LLMS, GBSS etc. related for performance and availability issues with EIS 2.0.
  a) This also entails attending the bridge calls initiated in the event of the incident and continuously providing the updates until the resolution is done.
  b) Given the criticality these calls must be attended, and resolutions are to be provided on a real time basis.

- **Service Desk Support –** Be the primary point of contact for all SD requests reported via SD portal etc.
  - **a.** Resolving service desk tickets assigned to module
  - **b.** Coordination with respective stake holders like Support Team, Bank Team, etc.
  - **c.** Processing Ad-hoc Request from bank
  - **d.** Preparing the daily reports

- **Application Support for the PR/DR site -** The team shall manage the routine and periodical DR drills, IBCE (Business Continuity) that the Bank undertakes.

- **Help Desk Requirements-** 24 * 7* 365 days per year, on-site and/ or on-line support facility as required.

- **Compliance and Audit Observation Closure –** The bidders has to arrange for timely clearances form Banks's Information Security Department (ISD), Enterprise & Technology Architecture (E&TA) Department for the project. The bidder has to ensure compliance with all guidelines of Central Govt., State Govt., RBI and Bank. All audit observations related to the project has to be closed within the stipulated timeframe by the bidder.

E2.8 INFRASTRUCTURE PROVIDED BY BANK

Table E-5 Infrastructure Provided by Bank

Sl No	Item	Details
1	Kubernetes based container Platform	Two container (Kubernetes) hosting platforms are available (a) RedHat OpenShift and (b) VmWare Tanzu. The bidder has to opt for only one of these two platforms. Components of both are listed below. **(a) Red Hat OpenShift** <u>Red Hat OpenShift Platform Plus with Runtimes:</u> OpenShift Plus: OpenShift Container Platform (x86_64 only), Broker/Master Infrastructure, Red Hat Advanced Cluster Management for Kubernetes, Red Hat Advanced Cluster Security for Kubernetes, Red Hat Quay Runtimes: JBoss Enterprise Application Platform (EAP), JBoss Web Server (JWS), JBoss Core Services, Red Hat Single Sign-On (SSO), Cloud Native Runtimes, Data Grid, AMQ (Broker only), Quarkus. <u>Red Hat Integration:</u> Red Hat Fuse, Red Hat AMQ, Red Hat AMQ streams, Red Hat 3scale API Management, Red Hat Change Data Capture, Red Hat Application Interconnect <u>Red Hat Ansible Automation Platform:</u>

		Automation Hub, Automation Mesh Any items which are not mentioned above will be provided by the Bidder at no additional cost to the Bank. **(b) VMware Tanzu** Spring Runtime: Enterprise support for spring packages VMware Tanzu Application Catalog: Custom-configured, pre-packaged open source application components Tanzu SQL: Enterprise support for MySQL and PostgreSQL Tanzu Build Service: Convert application source code into container images Tanzu Mission Control (On-Premise): Multi-Cluster Kubernetes management Tanzu Kubernetes Runtime: Enterprise Kubernetes Runtime Platform Tanzu RabbitMQ: Cloud Native Messaging and Streaming service Tanzu Gemfire: High performance Caching solution Any items which are not mentioned above will be provided by the Bidder at no additional cost to the Bank.
2	Bank's Private Cloud (ex: Meghdoot)	VMs with required numbers of Computes (cores), Memory and Storage provisioned in Bank's Private Cloud (ex: Meghdoot). Sizing needs to be provided by the Bidder.
3	Networking	Networking infrastructure
4.	Web Application Firewall	Centralised WAF (the successful bidder has to integrate the application with the centralised WAF.)
5	Database	Oracle Database Enterprise Edition Oracle Real Application Clusters Oracle Partitioning Oracle Advanced Security Oracle Database In-Memory Oracle Database Vault Oracle Advanced Compression Oracle Real Application Testing Oracle Multitenant Oracle Diagnostics Pack Oracle Tuning Pack Oracle Data Masking and Subsetting Pack Oracle Key Vault Oracle Data Integrator Enterprise Edition Oracle Business Intelligence Management Pack Oracle GoldenGate Oracle GoldenGate for Non Oracle Database Oracle Database Lifecycle Management Pack Oracle Audit Vault and Database Firewall

		Oracle Management Pack for Oracle Data Integrator Oracle Analytics Server or Oracle Business Intelligence Suite Extended Edition Oracle Management Pack for Oracle GoldenGate Oracle Managed File Transfer (#) Oracle GoldenGate for Big Data Targets (#) Oracle GoldenGate Veridata (#)
6	Enterprise-wide Cryptographic Key Management Solution	Features: Centralized key management. BYOK Azure BYOK AWS BYOK Tokenization (Vault less and Vault-based). Role Based Access. BYOE (Bring Your Own Encryption).
7	List of products available in Bank's private cloud platform (Meghdoot)	VMware Cloud Foundation VMware ESXi VMware Center Server NSX-T VMware Aria Operations for Logs VMware Aria Operations VMware Aria Automation VMware Aria Operations for Networks VMware Aria Suite Lifecycle VMware Live Site Recovery VMware vSphere Replication NSX Advanced Load Balancer Tanzu Kubernetes Grid

IMPORTANT NOTE:

1. Bidder to ensure that the necessary capacity, expertise, and capabilities for managing and supporting the infrastructure provided by the Bank.
2. Other software, tools, library, operating systems, appliances etc. that are required for the deliverables, has to be provided by the bidder. Details of such software, tools, appliances should be provided in Bill of Material (T.2 Bill of Material).
3. For any opensource tools / software / application / code / solution brought in by the Bidder, the same should be provided with Enterprise-Wide support for EIS 2.0 platform.
4. For the infrastructure provided by the Bank, Bidder needs to provide Sizing and specific details well in advance.

E2.9 OTHER ASPECTS

- Bidder to build EIS 2.0 as a cloud native application and to ensure that it can be migrated to any public cloud of Bank's choice with minimal effort.
- Bidder to provide Details of the licenses (along with calculation method/ formula) needed for all the products that are to be installed over the virtualization layer provided by SBI. Licenses (perpetual or otherwise) will be in the name of SBI.

- Bidder has to ensure that the architecture must be able to work in parallel with the existing architectures and manage the dependencies with them in a way that allows the new channels and the existing channels to work in parallel.
- Continuous upgrade, security patch deployment etc. of the platform/ application/ component (wherever available) will be Bidder's responsibility.
- The selected BIDDER should develop a disaster recovery plan for restoration of the system in the event of a disaster or major incident in line with the Bank's Policy and BCP. The Disaster Recovery (DR) Plan should be tested prior to the go-live as well as periodically, to verify DR readiness. Implement a disaster recovery approach, compliant with specific RPO and RTO metrics is Bidder's responsibility.

E3. DESCRIPTION OF DELIVERABLES

E3.1 EIS 2.0 Platform Deliverables

Some of the major principle capabilities and deliverables expected of EIS 2.0 are:

1. Deployment and Management: Deploy, install, maintain, and manage the Enterprise API Integration and Management Platform on SBI's private cloud infrastructure (ex: Meghdoot).
2. Microservices and Containerized Architecture: Create a containerized, microservices-based architecture with auto-scaling, self-healing, and service discovery capabilities.
3. Unified API Services: Provide unified API-based services, consolidating data and services from multiple downstream applications for consumption by various channels. Include SDKs and web-based integrations to accelerate adoption.
4. API Lifecycle Management: Implement comprehensive API lifecycle management, including standardization, version management, deprecation, and governance policies.
5. Event-Driven Architecture: Enable event-driven, asynchronous communication mechanisms to improve platform scalability and resilience.
6. Protocol Agnosticism: Support multiple communication protocols (e.g., REST, SOAP, GraphQL, WebSockets) to cater to diverse integration scenarios.
7. High Throughput Capability: Ensure the platform can handle a minimum of 8,000 TPS (Transactions Per Second) to meet enterprise-level demands.
8. Security and Compliance: Adopt enterprise-level API security (e.g., OAuth 2.0, JWT, encryption standards) and follow industry standards like Open Banking, BIAN, and PSD2.
9. Service Mesh Adoption: Utilize service mesh capabilities for high availability, fault tolerance, and traffic management within the microservices ecosystem.
10. Fault Tolerance and Resilience Patterns: Implement architectural patterns such as circuit breakers, retries, and throttling to enhance fault tolerance.
11. Error Handling and Message Mapping: Design a standardized error handling framework with well-defined error codes and messages for consistent API interactions.
12. Configurable API Parameters: Enable configurable performance parameters and timeout settings based on different API scenarios to optimize performance and response times.
13. Integrated Monitoring and Observability: Implement monitoring and observability capabilities to track resource availability, stability, and performance metrics.
14. Predictive Analytics and Proactive Response: Incorporate predictive analytics to identify potential issues and provide proactive responses, ensuring minimal service disruption.

15. End-to-End Traceability: Enable end-to-end customer interaction traceability, ensuring complete visibility into data flows and transaction histories.
16. ROC Integration: Interface with the ROC (Remote Operations Center) for enhanced observability and centralized monitoring.
17. Global Standards Adoption: Adhere to global standards such as Open Banking, BIAN, Swagger/OpenAPI for API specifications, and PSD2 compliance where applicable.
18. Multi-Channel Integration: Interface with various channels, including internal, external, and third-party service providers, as well as existing EIS systems.
19. Automation Capabilities: Implement automation features across application development, infrastructure provisioning, platform monitoring, and operational workflows to streamline operations.
20. Performance Optimization: Continuously optimize platform performance through automated load testing, scaling strategies, and resource management.

PLATFORM PERFORMANCE

Orchestrated and Individual APIs

Below is the projection of the number of APIs to be developed, configured and published by the Enterprise API integration and Management platform. The platform should be capable to host Orchestrated API as well as individual APIs.

Year-wise distribution is shown in below table:

Table E-6 Year-wise API Requirement

Years	Year 1	Year 2	Year 3	Year 4	Year 5
Orchestrated APIs	800	1400	1600	1800	2000
Individual APIs	1600	2800	3200	3600	4000

Though the year-wise orchestrated and Individual APIs are mentioned in the above table. However, the bidder has to provide unlimited licenses of all components which are part of the Integrated Product suite. The components of Integrated Product Suite should support development and publishing of orchestrated APIs above 2000 and Individual APIs above 4000 without any performance degradation and also without any additional cost to the bank during the contract period.

The number of resources onboarded by the bidder and OEM should be adequate to meet the scope of this RFP during the contract period.

THROUGHPUT

Definition of TPS:

Transaction: The number of API calls successfully executed, and effectively responded by the Enterprise API Integration and Management platform.

TPS (Transactions Per Second): The number of transactions successfully executed, and effectively responded by the Enterprise API Integration and Management platform per second.

As a part of the platform the bidder should have capability to measure the TPS as defined above.

The bidder has to ensure that the platform should support the following TPS capabilities:

Table E-7 Year-wise TPS Requirement

Years	Year 1	Year 2	Year 3	Year 4	Year 5
TPS	8000	9000	10000	11000	12000

However, the bidder has to augment components of Enterprise API Integration and Management platform to support any additional TPS requirements beyond 12000 without any performance degradation and also without any additional cost to the bank during the contract period.

Response Time

Transaction Processing Time: The time taken to completely process request by the platform, excluding the time taken by downstream systems to process and share the response. Transaction processing time = 100ms or less

Response Time = Platform processing time + Total time taken by all downstream systems

E3.2 ENVIRONMENTS

The selected bidder has to create the following regions:

Table E-8 Environments

S No.	Environment	No. of Instances
1.	Dev	1 region
2.	SIT	1 region
3.	UAT	3 regions
4.	Pre-Prod/ Regression Testing/ Performance	1 region
5.	PR	2 regions
6.	N-PR	1 region
7.	DR	2 regions
8.	N-DR	1 region

Please note that the application should be designed for all the Production (PR, DR, N-PR, N-DR) in active-active mode. (Initially PR and DR will be operational)

Tentative timelines for the above activities are mentioned in the "Milestones/Project Deliverables" section below.

E3.3 MILESTONES/PROJECT DELIVERABLES

The term of project is 5 years 0 months. Below is tentative timeline for Milestones/Project Deliverables:

Table E-9 Milestones/Project Deliverables

Phase	**Milestones/Deliverables**	**Timelines**
0	Issue of PO	P0
1	• Signing of SLA • Onboarding of architects and project leads • Finalization of Architectural diagrams, Network diagram, Design documents, Infrastructural needs (Based on this necessary infrastructure as mentioned in TABLE in E 3.9 INFRASTRUCTURE PROVIDED BY BANK will be provided by Bank)	P0+4 weeks

2	• Onboarding of all resources (including OEM) • Pre-clearance from Enterprise & Technology Architecture (E&TA) Department and ISD of Bank	P0+6 weeks
3	• Delivery and setup of platform, its applications, tools etc. for Dev, SIT and UAT • Successful setup of UAT (including post-clearance from E&TA Department and ISD of Bank) • Readiness of Production and DR environment	P0+8 weeks
4	• End-to-end delivery (including, but not limited to, development, orchestration design, development of business logic, if any, QA testing, ISD clearance, UAT Signoff and Go-Live in PROD and DR) of: • 5 services/ journeys from Retail list of APIs mentioned in Table E-1)	P0+12 weeks
5	• Complete DR Testing • End-to-end delivery (including, but not limited to, development, orchestration design, development of business logic, if any, QA testing, ISD clearance, UAT Signoff and Go-Live) of: • 15 of Remaining services/ journeys from the Retail list of APIs mentioned in Table E-1. • 10 services/ journeys from the corporate list of APIs mentioned in Table E-2. • Active-Active testing for PR and DR	P0+16 weeks
6	• End-to-end delivery (including, but not limited to, development, orchestration design, development of business logic, if any, QA testing, ISD clearance, UAT Signoff and Go-Live and DR) of: • 20 of Remaining services/ journeys from the Retail list of APIs mentioned in Table E-1. • 20 of services/ journeys from the corporate list of APIs mentioned in Table E-2.	P0+20 weeks
7	• End-to-end delivery (including, but not limited to, development, orchestration design, development of business logic, if any, QA testing, ISD clearance, UAT Signoff and Go-Live and DR) of: • Remaining services from retail banking category • 20 services from corporate banking category • 20 services from “other services” list such as wealth, insurance etc. mentioned in Table E-3.	P0+24 weeks
8	• End-to-end delivery (including, but not limited to, orchestration design, development of business logic, if any,	P0+32 weeks

	QA testing, ISD clearance, UAT Signoff and Go-Live and DR) of: • Remaining services from retail banking category • Remaining services from corporate banking category • Remaining services from Other services category.	

Details of three sets of journeys/ functionalities for EIS 2.0 are mentioned in **Section E2.5** of the RFP.

E3.4 PAYMENT TERMS

Please note – All amounts mentioned in the RFP should be in INR

Table T0: Payment Terms

Sr No	Cost Component	Amount
1	Project Deliverables (T1)	
2	Software Perpetual Licenses and ATS Cost (T2)	
3	Software Subscription Cost(T3)	
4	Resource Cost (T4)	
5	Training Cost (T5)	
	TOTAL	

Table T1: Project Deliverables

(Ref: Project Phases TABLE E 3.3 (point Milestones/Project Deliverables of Appendix- E))

Sl No	Milestones/Deliverables	Payment % of T1
1	After successful completion of Phase-1 and sign off by Bank	5%
2	After successful completion of Phase-2 and sign off by Bank	10%
3	After successful completion of Phase-3 and sign off by Bank	15%
4	After successful completion of Phase-4 and sign off by Bank	15%
5	After successful completion of Phase-5 and sign off by Bank	20%
6	After successful completion of Phase-6 and sign off by Bank	20%
7	After successful completion of Phase-7 & 8 and sign off by Bank	15%

Illustration:

Suppose total cost of project deliverables is INR 720.00, then amount paid to the successful bidder as per payment terms will as follows.

Sl No	Milestones/Deliverables	Payment % of T1	Amount to be paid
1	After successful completion of Phase-1 and sign off by Bank	5%	36
2	After successful completion of Phase-2 and sign off by Bank	10%	72
3	After successful completion of Phase-3 and sign off by Bank	15%	108
4	After successful completion of Phase-4 and sign off by Bank	15%	108
5	After successful completion of Phase-5 and sign off by Bank	20%	144
6	After successful completion of Phase-6 and sign off by Bank	20%	144

7	After successful completion of Phase-7 & 8 and sign off by Bank	15%	108
TOTAL			720

Table T2: Software Perpetual Licenses and ATS Cost

Sl No	Milestone	Payment Terms as a percentage of total Perpetual Licenses and ATS Cost
1	On completion of Production setup	20%
2	DR successful setup and testing	20%
3	Active-Active DC-DR rollout	20%
4	End of 2nd Year	10%
5	End of 3rd Year	10%
6	End of 4th Year	10%
7	End of 5th Year	10%
TOTAL		100%

Illustration: If the total cost of perpetual licenses and ATS is INR 500, then amount paid to the successful bidder as per payment terms will as follows:

Sl No	Milestone	Amount
1	On completion of Production setup	100
2	DR successful setup and testing	100
3	Active-Active DC-DR rollout	100
4	End of 2nd Year	50
5	End of 3rd Year	50
6	End of 4th Year	50
7	End of 5th Year	50
TOTAL		500

Table T3: Software Subscription Cost

Cost	Milestone	Payment Terms
1st year Subscription Cost	On completion of Production setup	40% of 1st year cost
	DR successful setup and testing	30% of 1st year cost
	Active-Active DC-DR rollout	30% of 1st year cost
2nd year Subscription Cost	At the end of 1st quarter of 2nd year	25% of 2nd year cost
	At the end of 2nd quarter of 2nd year	25% of 2nd year cost
	At the end of 3rd quarter of 2nd year	25% of 2nd year cost
	At the end of 4th quarter of 2nd year	25% of 2nd year cost
3rd year Subscription Cost	At the end of 1st quarter of 3rd year	25% of 3rd year cost
	At the end of 2nd quarter of 3rd year	25% of 3rd year cost
	At the end of 3rd quarter of 3rd year	25% of 3rd year cost
	At the end of 4th quarter of 3rd year	25% of 3rd year cost
	At the end of 1st quarter of 4th year	25% of 4th year cost
	At the end of 2nd quarter of 4th year	25% of 4th year cost

4th year Subscription Cost	At the end of 3rd quarter of 4th year	25% of 4th year cost
	At the end of 4th quarter of 4th year	25% of 4th year cost
5th year Subscription cost	At the end of 1st quarter of 5th year	25% of 5th year cost
	At the end of 2nd quarter of 5th year	25% of 5th year cost
	At the end of 3rd quarter of 5th year	25% of 5th year cost
	At the end of 4th quarter of 5th year	25% of 5th year cost

Illustration: If the total costs of subscription are INR 300, 200,200,200 and 200 for 1st, 2nd, 3rd, 4th, and 5th year respectively then amount paid to the successful bidder as per payment terms will as follows:

Cost	Milestone	Amount
1st year Subscription Cost	On completion of Production setup	120
	DR successful setup and testing	90
	Active-Active DC-DR rollout	90
2nd year Subscription Cost	At the end of 1st quarter of 2nd year	50
	At the end of 2nd quarter of 2nd year	50
	At the end of 3rd quarter of 2nd year	50
	At the end of 4th quarter of 2nd year	50
3rd year Subscription Cost	At the end of 1st quarter of 3rd year	50
	At the end of 2nd quarter of 3rd year	50
	At the end of 3rd quarter of 3rd year	50
	At the end of 4th quarter of 3rd year	50
4th year Subscription Cost	At the end of 1st quarter of 4th year	50
	At the end of 2nd quarter of 4th year	50
	At the end of 3rd quarter of 4th year	50
	At the end of 4th quarter of 4th year	50
5th year Subscription cost	At the end of 1st quarter of 5th year	50
	At the end of 2nd quarter of 5th year	50
	At the end of 3rd quarter of 5th year	50
	At the end of 4th quarter of 5th year	50
TOTAL		1100

Table T4: Resource Cost

NOTE:

- **The resource deployment and cost till PHASE-8 will be part of Project Deliverables (Appendix-E).** Adequate Resource deployment to be ensured by bidder to meet the project timelines till PHASE-8 without any additional cost to the bank.
- Details of the resource Role, KRAs, Role Experience & Qualifications etc. are mentioned in **Appendix-R.**

Resource Planning effective after completion of PHASE-8

		Resource planning to meet SLA

Resource Category	Per day resource cost (A) considering 22 days in a month	Shifts **	No of resources in a shift (B)	Total resources actually required (C)	Total of resources (D)	Total resource cost (A x D X 22)
L1		General				
		2 Shifts				
		3 Shifts				
L2		General				
		2 Shifts				
		3 Shifts				
L3		General				
		2 Shifts				
		3 Shifts				
Total for the Month (**E**)						
TOTAL FOR T4 = E x **actual number of months after phase 8**						

Please note:

1. **Bidder needs to plan for adequate number of resources to meet the scope of RFP. This number has to be provided in "Column D".**
2. **Then after if any additional resources are required to meet the scope of RFP, other than those quoted in the above table, will have to be provided by the bidder at no additional cost to the bank.**
3. **Payment will be made on actual number of resources deployed OR the number quoted in the Bid whichever is less.**
4. **Payment will be made on monthly arrears basis.**
5. **The minimum number of L1, L2 and L3 has to be 25, 25 and 8 respectively.**
6. **Bidders must ensure that 100% of the L3 and at least 70% of the L2 will be from OEM/ 3rd Party OEM.**
7. **Please refer to Appendix-R for Role, KRAs, Role Experience & Qualifications.**

***General Shift is from 10.00am to 6.00pm. (as per Bank working days in Mumbai)*
2 Shifts is from 06.30am to 2.30pm and from 02.30pm to 10.30pm (all days in a year)
3 Shifts is from 06.30am to 2.30pm and from 02.30pm to 10.30pm and 10.30pm to 6.30am (all days in a year)

Resource cost will be calculated as per the above table and will be paid monthly in arrears for the duration of the project.

Illustration:

Resource Category	Per day resource cost (A) considering 22 days in a month	Resource planning to meet SLA				
		Shifts	No of resources in a shift (B)	Total resources actually required (C)	Total of resources (D)	Total resource cost (A x D X 22)
L1	100.00	General	1	2	15	33,000.00
		2 Shifts	3	8		
		3 Shifts	1	5		
L2	110.00	General	3	4	17	41,000.00

		2 Shifts	2	5		
		3 Shifts	2	8		
L3	120.00	General	3	4	7	18,480.00
		2 Shifts	1	3		
		3 Shifts	0	0		
Total for the Month (E)						92,620.00
TOTAL FOR T4 = E x **actual number of months after phase 8 (for e.g. 52)**						48,16,240.00

Table T5: Training Cost

Year	No of participants per batch	No of batches per year	Cost per batch	Annual Cost (INR)
1	15	4		
2	15	4		
3	15	4		
	TOTAL			

Illustration:

Suppose total cost of training per batch is 27, then amount paid to the successful bidder as per payment terms will as follows.

Year	No of participants per batch	No of batches per year	Cost per batch	Annual Cost
1	15	4	27	108
2	15	4	27	108
3	15	4	27	108
	TOTAL			**324**

E4. Third-Party Components

Any software/ library/ component/ appliance etc. other than the details mentioned in the "INFRASTRUCTURE PROVIDED BY THE BANK" (Table E-5) has to be brought by the Bidder to meet requirements given in this RFP.

E5. Warranty Term

The Enterprise API Integration and Management (EIS 2.0) platform should be supplied along with comprehensive warranty applicable for 12 months from the date of Go-live. The warranty would be comprehensive in nature and with back-to-back support from the OEMs. The product(s) warranty is against all defects or vulnerabilities arising out of faulty design, coding, implementation, materials and media workmanship.

E6. Annual Maintenance (AMC) Term

- Annual Maintenance for all components of Enterprise API Integration and Management Platform to fully meet requirements given in this RFP.
- Infrastructure Support and Management for Production and non-production environment including but not limited to -

a. OS Administration –

- OS installation/upgradation, Kernel Patching and upgradation.
- Disk space Management for Production, ST, UAT servers, storages, and backup devices.
- Starting and stopping, restarting of various production and non-prod servers whenever required with prior communication to associated stakeholders.
- SCD implementation
- Timely closure of VAPT, Audit observations and SOC incidents, providing RCA for windows environment related issues wherever demanded
- Enabling of Integration with SOC, ITAM, PIMS, SIEM, DAM etc.
- Maintaining and regularly updating of asset inventory
- Backup and restoration as and when required and compliance with Bank's policy as per guidance provided by EIS department.
- Security patching and upgrade
- User administration including user management.
- Performance tuning and optimization of OS resources.
- File system management and optimization
- Implementation of security controls and regulatory controls as per banks guidelines and audit guidelines.
- CPU/Disk Space, Memory, threads monitoring and control
- Maintaining system logs, cluster logs, process monitoring, Kernel parameter tuning, maintaining server health check.
- Starting and stopping of various production & non-Production servers whenever required.
- Migration and replication of the existing VM infra onto new physical hardware as well as building new infra for EIS applications.
- Installation/uninstallation of related applications/packages/agents and housekeeping of servers as and when required for meeting the various requirements like patching/upgradation.
- Coordination with associated OEM/Partner to maintain uptime of EIS 2.0 ecosystem.
- Issue analysis and timely closure of the Linux environment related issue with proper RCA.
- Coordination with various stakeholders within bank for smooth functioning of EIS 2.0 ecosystem.
- Any other OS support related activities as identified by EIS 2.0 dept. /Bank
- Take all necessary steps to ensure fully functional EIS 2.0 to meet all requirements of this RFP.

b. Database Administration -

- Database monitoring, health check-ups and analysis for reporting of issues challenges and areas of improvement.
- Database backup/ restoration and archiving related activities.
- Support for migration and promotion activities.
- Housekeeping activities like reorganizing index, tables, clearing of old files, archival of tables etc., monitoring delayed processes, extracting data/logs as required and purging data as requested.
- Addition of disk groups, ASM disks, and space in tablespace. Optimising the DB capacity and maintenance of space.
- Implementation of OEM recommendations

- Implement SCD (Secure Configuration Document) policies, VAPT controls and other controls recommended by bank time to time.
- DB Servers patching with latest security patches.
- DB version upgradation or degradation and complete data migration, End-to-end testing with all existing application as and when requested by the bank.
- Request based support like report generation, DML execution, patch application, SCD implementation, DR drill support, VAPT support etc.
- SOC incident Closure, DAM integration
- Timely escalation of the problems to Bank / OEM / SRs.
- Timely resolution of issues in Production, ST UAT and Dev environment and submission of database related RCA within three days of the Incident.
- Any other DB support related activities as identified by EIS 2.0 dept. /Bank
- Take all necessary steps to ensure fully functional EIS 2.0 to meet all requirements of this RFP.

c. VMware/ Load Balancer/API Gateway/Enterprise Service Bus/ and any other tools/components provided in Solution -

- Server administration for mentioned infrastructure including and not limited to,
- OS installation/upgradation Performance tuning, optimization, and maintenance as per the applicability.
- Installation, configuration and maintenance of all tools, components provided as part of solution
- Installation, configuration, maintenance, and monitoring of VMware virtualization environment (if proposed in solution).
- User administration including user management and role management for all the mentioned infrastructure.
- File system management and optimization.
- Implementation of security controls and regulatory controls as per banks guidelines and audit guidelines.
- CPU/Disk Space, Memory, threads monitoring and control.
- Starting and stopping of various production & non-Production servers and applications whenever required.
- Coordination and working with various stakeholders within bank for smooth functioning of EIS 2.0 ecosystem.
- Monitoring of resource consumptions of Load Balancer
- Taking Routine Backups of above-mentioned components and publishing the status report with bank provided backup solution which have ability to perform backup of the components.
- Daily report generation regarding the ecosystem and publishing.
- New configuration changes (add the node, Pool, Virtual server, monitoring, VLAN creation, etc.)
- Troubleshooting of issues in EIS 2.0 platform
- Implementation of SCD (Secure Configuration Document), VAPT and Other regulatory compliance related controls
- Configuration of service Dashboards and BI Dashboards as and when required
- Implement, configure, integrate and maintenance of all tools, components of EIS 2.0 and fine-tuning of the same on a regular basis to ensure SLAs of EIS 2.0 are met.

- Upgradation, Housekeeping and Resolution of Infrastructure related issues.
- Any other related activities as identified by EIS 2.0 dept. /Bank
- Implement security with SSL, AAA (authentication, authorization, and accounting) services, Encryption, Decryption and OAuth 2.0 on different components of EIS 2.0.
- Manage user roles and permissions in EIS 2.0.
- Dash boarding and alerting mechanism for all devices and applications wherever applicable.

Take all necessary steps to ensure fully functional EIS 2.0 to meet all requirements of this RFP.

d. Help Desk Requirements

- 24 * 7* 365 days per year, online support facility.
- The expected time of resolution is given in Appendix for Service Level Agreement of this document.
- Escalation process should be in place for unresolved issues.
- Bidder support staff should be well trained to effectively handle queries raised by the Bank customer / employees etc
- Bidder should have ability to generate MIS reports periodically for example: Volume of calls / per day, resolution % per day, other parameters as required in ROC, regulatory reporting requirements etc. Reports related requirements expected at this point of time are given in the subsequent appendix of this RFP. However, Bank will share MIS related requirements with selected bidder from time to time during tenure of this contract which bidder needs to fulfill.
- Support to channels and Operations - This involves attending to the IT requests, incident as per the incident management policy, calls, mails, and queries on 24x7x365 basis from various channels/departments like YONO, RLMS, FIGS, ATM, UPI, PSG, CMP, LLMS, GBSS etc. related for performance and availability issues with EIS 2.0. This also entails attending the bridge calls initiated in the event of the incident and continuously providing the updates until the resolution is done. Given the criticality these calls must be attended, and resolutions are to be provided on a real time basis

e.Service Desk Support

Be the primary point of contact for all SD requests reported via SD portal etc.

- Resolving service desk tickets assigned to module
- Coordination with respective stake holders like Support Team, Bank Team, etc.
- Processing Ad-hoc Request from bank
- Preparing the daily reports

f.Application Support for the PR/DR site

The team shall manage the routine and periodical DR drills, IBCE that the Bank undertakes. Also, team should handle PR <-> DR switch over in case of emergency situation to meet availability requirements of EIS 2.0.

E7. MIS Report Generation requirement

- Indicative reports related requirements expected at this point of time are given in the subsequent appendix of this RFP. However, Bank will share MIS-related requirements with selected bidders during tenure of this contract which bidder must fulfill.
- Generation of execution/ performance/ noncompliance/ exceptional/ deletion history/ audit reports and audit trails desired by the Bank. Customization of existing reports/creation of new reports. Interactive dashboards with provision to further drill down the reports.
- End to end API observability along with prediction of API failures based on past trends.

E8. In case of Transaction System

1. Audit trail requirement: Audit logging of 100% of transactions must be ensured for all legs of API calls.
2. Audit logs reporting & analysis tool
3. Solution should support TPS as provided in Table E-6.

E9. Performance Requirements

The bank has defined metrics that the bidder must adhere to. The metrics may need to be fulfilled earlier in case of faster-than-expected growth. In such a case, bidder must ensure they can scale the app / infra appropriately and in a timely manner. Each technology proposed by the bidder should sustain the requirements as defined below for storage, processing, and delivering the outcome to customers.

Table E-11 Performance Projection

Category	Metric Details	Requirements
Volumetrics	**Number of APIs** Defined as the APIs being utilized by the multiple channels to undertake various banking (financial and non-financial) transactions. The number of current APIs has been determined by considering existing APIs of various channels such as YONO, RINB, CINB, YONO Business etc. which includes some APIs already hosted on EIS 1.0. The projected numbers have been determined basis bank's growth rate across multiple banking channels.	**Current:** 1000-2000 **Short-term projected (3-5 Years):** 2000-3000 **Long-term projected (6-10 Years):** 4000-5000

	Number of transaction requests/minute Defined as the number of transaction (financial and non-financial) requests coming in from multiple channels into the core systems every minute A transaction is defined as a request originated by a user on a particular channel (YONO, INB etc.) to fulfil one functionality (e.g. PIN change, balance enquiry etc.) The number of current transaction requests/minute has been determined by considering transaction volumes across multiple channels along with various payment systems such as NEFT, RTGS, IMPS and UPI The projected numbers have been determined basis bank's growth rate across multiple banking channels and payment systems.	**Current:** 2.0-2.5 million/minute **Short-term projected (3-5 Years)** 6-7 million/minute **Long-term projected (6-10 Years):** 13-15 million/minute

- Uptime requirement of 99.99% for Production Environment.
- Uptime requirement for Non-Production Environments as mentioned in the **Appendix-J**.
- API processing must be maintained within 100 ms of the base response time within EIS 2.0 ecosystem of all transactions being received from upstream applications at EIS 2.0 via API route. This will exclude the third-party/other application's response time, i.e. downstream applications.
- Management and fixing of the Incidents to be done as per the table below:

Table E-12 Incident Management

<table>
<tr><th>Category</th><th>Key metrics</th><th colspan="3">Definition</th><th>Requirements (to be fixed in)</th></tr>
<tr><td rowspan="5">Incident Management</td><td rowspan="5">Root cause resolution (Mean Time to Resolve)</td><td>Severity</td><td>Urgency</td><td>Impact</td><td rowspan="5">Severity1:1hr
Severity2:4hrs
Severity3:12hrs
Severity4:48hrs
In addition, ensure minimization of the number of incidents and service errors per month, through stringent quality checks and resilience</td></tr>
<tr><td>1</td><td>Immediate / Critical</td><td>Extensive/Widespread/ Regulatory mandate</td></tr>
<tr><td>2</td><td>High</td><td>Significant/Large</td></tr>
<tr><td>3</td><td>Medium</td><td>Moderate/Limited</td></tr>
<tr><td>4</td><td>Low</td><td>Minor/Localized</td></tr>
</table>

			measures. Month-on-month or quarter-on-quarter incidents are to be tracked and limits are to be defined as part of SLAs

E10. Scalability Requirements

All components of the solution must support scalability to provide continuous growth to meet the Bank's requirements and demands. The solution should scale and behave consistently with growth in data, number of concurrent sessions, etc. SBI has high expectations in terms of volume due to the constant increase in the baseline of customers and in the number of functionalities.

E11. Regulatory / Compliance Requirements

- The BIDDER must ensure that the EIS 2.0 ecosystem adheres to all the governing laws and guidelines pertaining to technology, data security, consent management, etc. as defined by the Bank and relevant regulatory authorities (e.g., RBI, FIU, all NPI, IT act, data privacy act (GOI) etc.).
- The BIDDER must work with relevant SBI teams and stakeholders to ensure that all the journeys are designed, developed, and implemented in line with all the existing regulatory and compliance requirements.
- The BIDDER is mandated to incorporate all the ad-hoc regulatory demands as generated by the Bank or regulatory authorities within the stipulated time (e.g., RBI digital payment system control).
- The BIDDER must create a future-proof platform that envisages potential regulatory changes and ensures a flexible build to incorporate such changes in the shortest time possible.
- Bidder, on behalf of EIS 2.0, has to provide on-demand logging and reporting that could potentially be used for audit compliance and legal purposes.
- The BIDDER to prevent, detect and address any nonconformity or deviation from applicable laws and guidelines during the execution of the project.
- All the performance parameters reports should be system generated and submitted monthly or as requested by the bank.

E12. Security Requirements

SECURITY

All security requirements as enforced by IS department of the Bank must be implemented properly by selected bidder. A non-exhaustive sample of security requirements across key areas are provided below:

General:

- The Bidder's/ OEM security compliance would be attained during the bid process in writing, and its responses will be verified post-onboarding.
- All employees of the OEM must be made aware of and trained in the security guidelines to be maintained during the platform design, development, and deployment. They will also sign confidentiality agreements and NDA at a company level.
- After the OEM, SBI and the partner consultants of SBI finalize the architecture, threat modelling would be conducted, and a security plan developed including:
  - ✓ Recommendations on the architecture/ design.
  - ✓ Development process, secure coding, and code security guidelines.
  - ✓ API security, OS / Web/ Database/Middleware/End point security requirements.
  - ✓ Data security Data flow / DFD process, Encryption requirements, Document security, Data leak possibilities.
  - ✓ Milestones for when ISD will conduct security checks to ensure the process is in line.
- The OEM must ensure a secure development life cycle during product development and adhere to the following guidelines:
  - ✓ Developers are trained on secure coding practices
  - ✓ Code testing is performed using SAST tools
- The OEM must participate in all milestones-based checks by ISD and comply with the direction provided by the ISD team.

Secure Design:

- Develop, implement, maintain and use best in class industry proven security controls and industry standards such as OWASP, SANS, NIST frameworks during design and development phase.
- The OEM must ensure and incorporate all necessary security and control features within the application, OS, database, network etc., as per OWASP, SANS standards to maintain confidentiality, integrity and availability of the data and systems.
- The platform should support strong authentication controls like multifactor authentication.
- The platform should have strong authorization controls. User and admin access control management to be provided as part of solution. Access control to be based on least access privilege principle.
- Solution to have controls for prevention against unauthorized data access and distribution. SBI or team assigned by SBI will be reviewing all access controls mechanism defined.
- The solution should be capable of integrating with the existing single sign on facility of the Bank.
- The solution to have strong file level validation controls for size, type and content with preventive control against malware using controlled sandbox environment.

- The file store locations need to be secured using industry standard strong cryptographic controls such as FIPS-140, level 2.
- The encryption should support data while in transit or rest. All encryption keys should be stored in secured location (such as HSM) with limited access as per NIST framework.

Secure development:

- The solution should adhere to the S-SDLC (Secure System Development guidelines.
- The OEM to adhere to the security plan as per the S-SDLC activities and should incorporate it into the Project Plan before getting it approved from the Bank Developers should be skilled in secure coding and OWASP Top ten, SANS 25 vulnerabilities.
- Code should be developed as per secure coding practices and reviewed to ensure the same. Any product-level security observations should be resolved in a maximum of 3 months (for all criticalities).
- Isolated sandbox environment with appropriate scanning, processing & validation features for preventing any malicious content/code before being sent to internal system.
- All the hardware or required components should be shipped directly from OEM to the bank's premises.
- OEM should enforce process and policies such that only authorized users should have access to the source code. Test data should not be sourced from production/internal data of the Bank without implementing appropriate controls and due approvals from the Bank.
- The source code should be maintained in a version-controlled environment that provides for logging and audit of all activities performed on source code.
- Development, testing, staging and production environment must be physically and logically separated from one another.
- The solution should ensure there should be no data leakages by implementation of distributed programming frameworks.
- The solution should secure data storage and logs. Auditing should be enabled to track each activity.
- All the underlying infrastructure components such as OS, servers (web, application, and database) or any product should policy on each environment before being made functional.
- Logging should be defined properly to be able to carry out forensics of incidents whenever required or as need arises.
- OEM should provide the support for integration of the application with Web Application Firewall (WAF), IDS, IPS, SIEM, DAM, etc. and provide the requisite details to concerned Teams for implementation of the same.

Secure Assessment:

- Wherever applicable, the OEM to conduct SAST (Static Application Security Testing) & DAST (Dynamic Application Security Testing) and provide detailed reports of the same within timelines as specified by the Bank or the Bank may conduct the security assessment of the same. The OEM should close all the vulnerabilities which should be validated by conducting SAST & DAST again.

- The OEM should provide full support to Security Review, VAPT and Risk Assessment of all platforms conducted by SBI.
- Standards Benchmark - To ensure that all parties have a common understanding of any security issues uncovered, the independent organization that specializes in Information security shall provide a rating based on industry standards as defined Weakness Enumeration (CWE).

Secure use of Open Source:

- The Implementation of open-source technologies should be taken up in compliance with the policy of the Bank.
- The OEM provides full support in implementation and maintenance for the opensource technologies in terms of upgradation, patching, etc.
- The OEM should provide the list of all open-source libraries being used on the platform. All such libraries/code should undergo SAST to verify the absence of any malicious code/script.
- OEM shall disclose all binary executables (i.e., compiled or byte code; source code is not required) of the software, including all libraries or components.
- OEM shall disclose the origin of all software and hardware components used in the product including any open source or 3rd party licensed components.

Security compliance to policies and process:

- The OEM shall abide by the access level agreement to ensure safeguards of the confidentiality, integrity, and availability of the information systems. OEM will not copy any data obtained while performing services under this RFP to any media, including hard drives, flash drives, or other electronic devices, other than as expressly approved by the Bank.
- The Bank will have right to audit the OEM's people, processes, technology, etc. as part of the OEM security risk assessment process.
- Solution should also be compliant to ISO27001 controls, Indian Information Technology Act, 2000 (along with amendments as per Information Technology (Amendment) Act, 2008) and any applicable data privacy & protection Act.
- All engaged personnel/Resources should agree to the terms and conditions of NDA and sign in with the Bank.

Security for support and maintenance:

- OEM should follow all the processes defined by the Bank like Incident, Change, Release and Patch Management, etc.
- Static application security testing and dynamic application security testing should be conducted by the OEM for any change request involving a design or code change. All gaps identified will be fixed by OEM prior to go-live.
- The Bank reserves the right to conduct further security testing of the source code and the system by either the Bank personnel or another party. Any gaps identified during this testing will be fixed by OEM at no extra cost to the Bank.
- Configuration items such as computers and other devices, software & hardware contracts, and licenses, third party tools and business services, related to the application to be disclosed.
- OEM will resolve security incidents as per the agreed SLAs.

- All user and technical access will be granted as per the Role Based Access Control (RBAC) matrix approved by the Bank. All access will be reviewed as per defined frequency and during control points e.g., when a team-member leaves team or organization.
- Information Security controls will be enforced when moving production data into non-production environments with only due approvals e.g., masking/anonymize sensitive data during the cloning process etc. Audits will be conducted by the Bank to ensure security controls sustenance. Any gaps identified will be remediated by the OEM before data movement.
- OEM to provide appropriate evidence of their security status and ability to meet minimum security requirements of Bank throughout the various stages of the contract competition.

In addition, following requirements are to be met by bidder –

1. Rendering assistance to EIS 2.0 Department for any internal / external Audit and Security Reviews conducted by ISD / Third Party. Timely resolution of observations during Audit / Security Reviews.
2. Support for SCD, Internal SCD, External Audits, Security Reviews and IT Risk related activities
3. SCD review and changes based on existing and revised Bank guidelines under guidance of EIS department.
4. SCD Hardening (OS/DB, Closure of VA-PT Observations) for all alerts of EIS Department.
5. All IT-RISK /IS-Audit and any other security related activities in EIS for closure of VAPT under the guidance of EIS department.
6. Maintaining system logs

E13. Limited Trial / Pilot Requirements

Successful deployment of two orchestrated journeys / applications identified by the Bank to verify the expected benefits.

E14. Review and Testing; Acceptance

Tools to perform performance testing of the EIS 2.0 platform and evaluating the performance in terms of responsiveness and stability under certain workloads. The Bank is currently using JMeter for automated performance testing. The BIDDER has to bring in the expertise and continue using JMeter for conducting automated performance testing of EIS 2.0. The BIDDER has to conduct extensive performance testing before each product release.

E15. Backup system / POC / test & training system / DR system

E16. Training

The selected bidder is expected to conduct relevant platform related training for Bank staff, four batches in one year with batch strength of 15 persons per batch for three years from the start of the project.

Table E–13 Training Batches

Year	No of participants per batch	No of batches per year
1	15	4
2	15	4
3	15	4

Appendix-F

Commercial Bid

The Commercial Bid needs to contain the information listed hereunder and needs to be submitted on portal of e-Procurement agency**.**

Please note – All amounts mentioned hereunder has to be in INR only.

Name of the Bidder:

Sr No	Cost Component	Amount
1	Project Deliverables (F1)	
2	Software Perpetual Licenses and ATS Cost (F2)	
3	Software Subscription Cost (F3)	
4	Resource Cost (F4)	
5	Training Cost (F5)	
	TOTAL (This will be the Total Cost of Ownership (TCO)/Total Project Cost)	

Table F1: Project Deliverables

(Ref: Project Phases TABLE E 3.3 (point Milestones/Project Deliverables of Appendix - E))

Sl No	Deliverables	Amount
1	Total cost of Deliverables	

Tables F2: **Software Perpetual Licenses and ATS Cost**

(For Software /Components /Tools proposed by the bidder with perpetual licenses)

Sl No	Software /Components /Tools Name	OEM Name	Perpetual license cost
1			
2			
3			
4			
5			
6			
		TOTAL F2	

Note:

1. Any software/ library/ component/ appliance etc. other than the details mentioned in the "INFRASTRUCTURE PROVIDED BY THE BANK" (Table E-5) has to be brought by the Bidder to meet requirements given in this RFP.
2. Bank may decide to procure licenses for some OR all of the products mentioned in the above list. PO will be issued only for the actual procurement of Product / Software / Component required & decided by the Bank.

3. Licenses should be in the name of State Bank of India by OEM.

Tables F3: **Software Subscription Cost**:

(For software /components /tools proposed by the bidder on Subscription basis)

Sl No	Software /Components /Tools Name	OEM Name	Subscription cost for					Total for 5 years
			1st Year	2nd Year	3rd Year	4th Year	5th Year	
1								
2								
3								
4								
5								
6								
Total for the Year								
TOTAL F3								

Note:

1. Bank may decide to procure licenses for some or all of these products mentioned in the above list. PO will be issued only for the actual procurement of Product / Software / Component required & decided by the Bank.
2. Licenses should be in the name of State Bank of India by OEM.
3. Any software/ library/ component/ appliance etc. other than the details mentioned in the "INFRASTRUCTURE PROVIDED BY THE BANK" (Table E-5) has to be brought by the Bidder to meet requirements given in this RFP.

Table F4: Resource Cost

Resource Planning effective after completion of PHASE-8

Resource Category	Per day resource cost (A) considering 22 days in a month	Resource planning to meet SLA				
		Shifts **	No of resources in a shift (B)	Total resources actually required (C)	Total of resources (D)	Total resource cost (A x D X 22)
L1		General				
		2 Shifts				
		3 Shifts				
L2		General				
		2 Shifts				
		3 Shifts				
L3		General				
		2 Shifts				
		3 Shifts				
Total for the Month (E)						
TOTAL FOR F4 = E x **52 months**						

Please note:

1. **Bidder needs to plan for adequate number of resources to meet the scope of RFP. This number has to be provided in "Column D".**
2. **Then after if any additional resources are required to meet the scope of RFP, other than those quoted in the above table, will have to be provided by the bidder at no additional cost to the bank.**
3. **Payment will be made on actual number of resources deployed OR the number quoted in the Bid whichever is less.**
4. **Payment will be made on monthly arrears basis.**
5. **The minimum number of L1, L2 and L3 has to be 25, 25 and 8 respectively.**
6. **Bidders must ensure that 100% of the L3 and at least 70% of the L2 will be from OEM/ 3rd Party OEM.**
7. **Please refer to Appendix-R for Role, KRAs, Role Experience & Qualifications.**

***General Shift is from 10.00am to 6.00pm. (as per Bank working days in Mumbai)*
2 Shifts is from 06.30am to 2.30pm and from 02.30pm to 10.30pm (all days in a year)
3 Shifts is from 06.30am to 2.30pm and from 02.30pm to 10.30pm and 10.30pm to 6.30am (all days in a year)

Resource cost will be calculated as per the above table and will be paid monthly in arrears for the duration of the project.
Bidders must ensure that 100% of the L3 and at least 70% of the L2 will be from OEM.

Table F5: Training Cost

Year	No of participants per batch	No of batches per year	Cost per batch	Annual Cost
1	15	4		
2	15	4		
3	15	4		
	TOTAL F5			

Table F6: Breakup of Taxes and Duties

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

Name & Signature of authorised signatory

Seal of Company

Appendix-G

Certificate of Local Content

Date:

To,
_____
_____
_____

Dear Sir,

Ref.: RFP No.: _____ Dated: 14/10/2024

This is to certify that proposed _____ <product details> 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

Appendix–H

BANK GUARANTEE FORMAT

(TO BE STAMPED AS AN AGREEMENT)

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).

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 Software Solution/ Service) (hereinafter referred to as **"Services")** to SBI in accordance with the Request for Proposal (RFP) No. SBI/GITC/EIS2.0/2024-25/1221 dated 14/10/2024.

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

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 the 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.

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

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

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

1. 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.
2. 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.

3. 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.

4. This 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

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

6. 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.

7. 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:

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

2. This Bank Guarantee shall be valid upto_____

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

Yours faithfully,

For and on behalf of bank.

_____

Authorised official

Appendix-I

PROFORMA OF CERTIFICATE TO BE ISSUED BY THE BANK AFTER SUCCESSFUL COMMISSIONING AND ACCEPTANCE OF THE SOFTWARE SOLUTION/ SERVICES

Date:

M/s._____

_____

Sub: Certificate of delivery, installation and commissioning

1. This is to certify that the Software Solution as detailed below has/have been successfully installed and commissioned (subject to remarks in Para No. 2) in accordance with the Contract/specifications.

   - PO No._____ dated _____ ___
   - Description of the Solution _____
   - Quantity _____
   - Date of installation_____
   - Date of acceptance test _____
   - Date of commissioning _____

2. Details of specifications of Software Solution not yet commissioned and recoveries to be made on that account:

   S. No. Description Amount to be recovered

3. The installation and commissioning have been done to our entire satisfaction and staff have been trained to operate the Software Solution.

4. Service Provider has fulfilled his contractual obligations satisfactorily

or

Service Provider has failed to fulfill his contractual obligations with regard to the following:

(a)

(b)

(c)

5. The amount of recovery on account of non-supply of Software Solution/Services is given under Para No. 2 above.

Signature _____

Name _____

Designation with stamp _____

_____

Appendix-J

Penalties

PENALTY FOR NON-PERFORMANCE:

Product delivery:

Table J-1 Product delivery

Sr No	Metrics	Threshold	Penalty
1	Percentage of milestones delivered on time	100% of milestones should be delivered by as stated.	Delay >= 1 week - 1% of the milestone cost for each month (and/ or part thereof) till 4 weeks, beyond 4 weeks of delay 10% of the milestone cost.

Availability:

Table J-2 Availability

Sr No	Metrics	Threshold	Penalty for shortfall
1	Uptime of Pre-Prod environment	99.0%	Downtime of each 1% or part thereof, beyond 99% - Penalty 1% of the respective Monthly Project delivery/ Resource cost as the stage may be. (max – 5% Penalty of Monthly Project delivery/ Resource cost as the stage may be).
2	Uptime of non-prod environments	Dev environment: 95% SIT environment: 95% UAT environment: 99%	Downtime of each 5% or part thereof, beyond 95% - Penalty of 1% for of Monthly Project delivery/ Resource cost as the stage may be. (max – 5% Penalty of Monthly Project delivery/ Resource cost as the stage may be).
3	Uptime of the Prod environments and Prod monitoring tools	99.99%	Downtime of each 0.01% or part thereof, beyond 99.99% - Penalty of 2% of the respective Monthly Project delivery cost and/ or part thereof. (max – 10% of Penalty of the respective Monthly Project delivery cost) (Till Phase-8. After Phase-8 please refer to Penalties for SLA uptime given below)
4	RTO (Recovery Time Objective)	Up to 5 minutes	Delay beyond each 5 minutes or part thereof - 1% of the respective Monthly Project delivery/ Resource cost as the stage may be. (max - 5%

			Penalty of the respective Monthly Project delivery/ Resource cost).
5	RPO (Recovery Point Objective)	0 minutes	10% of the respective Monthly Project delivery/ Resource cost as the stage may be.

Environment Setup:

Table J-3 Environment Setup

Sr No	Metrics	Threshold	Penalty
1	Time to environment setup Prod Pre-Prod Non-Prod (Dev, SIT, UAT)	Phase date	Delay of >= 1 week: Penalty of 1% of the Phase-wise cost for each week delay till 4 weeks (and/ or part thereof). Beyond 4 weeks of delay: 10% of the Phase-wise cost.
2	DevSecOps and design tools setup	Phase date	Delay of >= 1 week: Penalty of 1% of the Phase-wise cost for each week delay till 4 weeks (and/ or part thereof). Beyond 4 weeks of delay: 10% of the Phase-wise cost.
3	Monitoring setup across environment Prod Pre-Prod Non-Prod (Dev, SIT, UAT)	Phase date	Delay of >= 1 week: Penalty of 1% of the Phase-wise cost for each week delay till 4 weeks (and/ or part thereof). Beyond 4 weeks of delay: 10% of the Phase-wise cost.

Security and Compliance:

Table J-4 Security and Compliance

Sr No	Metrics	Threshold	Penalty for deviation/breach
1	Time to resolve Production vulnerabilities detected.	Critical: 1hr High severity: 4 hrs Medium severity: 12hrs Low severity: 48hrs	2% of the monthly cost and/ or part thereof for each instance of: 1hr delay for Critical severity 4hrs delay for High severity 12hrs delay for Medium severity 48hrs delay for Low severity (max 10% of the monthly cost)
2	Level of compliance with regulatory/legal requirements	100% compliance with regulatory/legal requirements	2% of the monthly cost and/ or part thereof for each 5 days delay for non-compliance. (max 10% of the monthly cost)
3	Closure of Audit observations related to the project.	Within 7 days of its intimation from Bank	0.1% of total cost of the respective "Project Deliverables" Phase, per day of delay after threshold and/ or part thereof with maximum of 1% of total "Project Deliverable" cost Or

			1% of "Monthly Resource Cost" per day of delay and/ or part thereof depending on the phase of the project with a maximum of 10%.

Penalties for SLA Monthly uptime shall be as under (PROD Environment):

Table J-5 Production Uptime

S No	Uptime Range (Monthly)	Penalty
1	99.90% to below 99.99%	1% of operational monthly invoice amount for each instance for every defaulting month and/ or part thereof.
2	99.80% to below 99.90%	2% of operational monthly invoice amount for each instance for every defaulting month and/ or part thereof.
3	99.70% to below 99.80%	3% of operational monthly invoice amount for each instance for every defaulting month and/ or part thereof.
4	99.60% to below 99.70%	4% of operational monthly invoice amount for each instance for every defaulting month and/ or part thereof.
5	99.50% to 99.60%	5% of operational monthly invoice amount for each instance for every defaulting month and/ or part thereof.
6	Below 99.50%	Beyond 30 minutes of downtime: 5% of monthly invoice amount for each instance for every defaulting month (max 30% of operational monthly invoice amount)

Penalty for Project Governance

Table J-6 Project Governance

Sl No.	SLA Measure /Parameter	Description	Target	Penalties/Liquidation Damage
1	Management Summary submission	Fortnightly submission of problem management summary	No delay	Nil
			Delay up to 3 days	1% of the Monthly billing of Project Governance & Management team for each instance of 3 days delay.
			Every one-week delay beyond 3 days	5% of the Monthly billing of Project Governance & Management team for each instance of 1 week delay and/ or part thereof. (max-20%)
2	KEDB Update	Maintain and Update KEDB	100 %	0% of the Monthly billing of Project Governance & Management team and/ or part thereof.

		within 3 days as per SLA	95% and above	1% of the Monthly billing of Project Governance & Management team for each instance of 3 days delay. (max 10%)
			Less than 95%	5% of the Monthly billing of Project Governance & Management team for each instance of 3 days delay. (max 15%)
3	RCA of Incidents	RCA Submission for incidents as per SLA	No delay	Nil
			Delay up to 3 days	1% of the Monthly billing of Project Governance & Management team for each instance of 3 days delay and/ or part thereof. (Max 10% of the Monthly billing of Project Governance & Management team)
			Every one-week delay beyond 3 days	5% of the Monthly billing of Project Governance & Management team for each instance of 1 week delay and/ or part thereof. (max 15% of the Monthly billing of Project Governance & Management team)

Penalty for Governance & Compliance SLAs

Table J-7 Governance & Compliance

Sl No.	SLA Measure /Parameter	Description	Target	Penalties/Liquidation Damage
1	SOP Compliance	Number of instances of SOP non-compliance	Zero	Nil
			Up to 2	1% of the Monthly billing amount of Project Manager and/ or part thereof.
			More than 2	5% of the Monthly billing amount of Project Manager Additional 1% for each instance if non-compliance beyond 2 instances and/ or part thereof.
2	Report submission on SOPs	Quarterly report submission on SOPs and their modification status	No delay	Nil
			Delay of up to 15 days	1% of the Monthly billing amount of Project Manager.
			Delay beyond 15 days	5% of the Monthly billing amount of Project Manager and/ or part thereof.
3	Report submission	Quarterly report submission	No delay	Nil
			Delay of up to 15 days	1% of the Monthly billing amount of Project Manager.

	on Architecture	on Architecture improvement and initiatives	Delay beyond 15 days	5% of the Monthly billing amount of Project Manager and/ or part thereof.
4	Report submission on Project Delivery	Monthly report submission of project health and delivery	No delay	Nil
			Delay of up to 10 days	1% of the Monthly billing amount of Project Manager.
			Delay beyond 10 days	5% of the Monthly billing amount of Project Manager and/ or part thereof.
5	Report submission on Deployments	Monthly submission of UAT to production deployment progress report	No delay	Nil
			Delay of up to 10 days	1% of the Monthly billing amount of Project Manager.
			Delay beyond 10 days	5% of the Monthly billing amount of Project Manager and/ or part thereof.

Penalty for Testing SLAs

Table J-8 Penalty for Testing

Sl No.	SLA Measure /Parameter	Description	Target	Penalties/Liquidation Damage
1	FTR in UAT	First Time Right in UAT (FTR). For each UAT failure, UAT team shall provide the list of business scenarios which were Passed, Failed and could not be tested. For the Deliverables /CRs if any changes are suggested during testing cycles, fresh tracking will start from date of approval of	90% and above	Nil
			80% to less than 90%	10% of the billed amount of the Deliverables / CR during billing month If any Deliverables / CRs failed more than 3 times due to code/ package issue additional penalty of 10 % will be charged over and above the penalty charged for FTR.
			50% to less than 80%	20% of the billed amount of the Deliverables / CR during billing month If any Deliverables / CRs failed more than 3 times due to code/ package issue additional penalty of 10 % will be charged over and above the penalty charged for FTR.
			25% to less than 50%	30% of the billed amount of the Deliverables / CR during billing month If any Deliverables / CRs failed more than 3 times due to code/

		revised approach.		package issue additional penalty of 10 % will be charged over and above the penalty charged for FTR.
			Less than 25%	40% of the billed amount of the Deliverables / CR during billing month If any Deliverables / CRs failed more than 3 times due to code/ package issue additional penalty of 10 % will be charged over and above the penalty charged for FTR.
2	Load / regression testing	Timely submission of report for load testing of critical API	No Delay	Nil
			Delay of up to 15 days	2% of the Monthly billing of regression testing resources
			Delay beyond 15 days	5% of the Monthly billing of regression testing resources for each week of delay and/ or part thereof. (max 15%)
3	ST Ageing – Turnaround time	ST clearance of 80% of Deliverables /CRs promoted in month	No Delay	Nil
			Delay of up to 15 days	2% of the Monthly billing of regression testing resources
			Delay beyond 15 days	5% of the Monthly billing of regression testing resources for each week of delay and/ or part thereof. (max 15%)

Penalty for Incident Management (Severity as defined in Table E-12)

Table J-9 Incident Management

Sl No.	SLA Measure /Parameter	Description	Target	Penalties/Liquidation Damage
1	Severity 1 level incidents	Count of Severity level 1 incidents	Zero	Nil
			1	2% of Monthly billing amount of Total resources cost.
			More than 1	5% of Monthly billing amount of Total resources cost for each severity level 1 incident.
2	Severity level 1 incidents	Severity level 1 incidents acknowledged and resolved as per the threshold acknowledgement	100%	Nil
			Greater than 95%	2% of Monthly billing of Total Resource cost.
			95% or below	5% of Monthly billing of Total Resource cost and/ or part thereof.

		and resolution time SLA for Severity 1		
3	Severity level 2 incidents	Severity 2 level incidents acknowledged and resolved as per the threshold acknowledgement and resolution time SLA for Severity 2 level incidents	100%	Nil
			Greater than 90%	2% of Monthly billing of Total Resource cost.
			90% or below	5% of Monthly billing of Total Resources cost and/ or part thereof.
4	Severity level 3 and 4 incidents	Severity 3 and Severity 4 level incidents resolution. Severity 3 and Severity 4 level incidents to be acknowledge and resolved as per the threshold acknowledgement and resolution time SLA for Severity 3 and Severity 4 level incident	100 %	Nil
			Greater than 95%	2% of Monthly billing of Total Resources cost and/ or part thereof.

Appendix-K

Service Level Agreement

BETWEEN

STATE BANK OF INDIA

AND

_____

Commencement Date:

Date of Expiry:

This agreement ("Agreement") is made at_____ (Place) on this _____day of _____ 201_.

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,[1] hereinafter referred to as "**the Bank**" which expression shall, unless it be repugnant to the context or meaning thereof, be deemed to mean and include its successors in title and assigns of the First Part:

AND

_____[2] a private/public limited company/LLP/Firm <*strike off whichever is not applicable*> incorporated under the provisions of the Companies Act, 1956/ Limited Liability Partnership Act 2008/ Indian Partnership Act 1932 <*strike off whichever is not applicable*>, having its registered office at …….. hereinafter referred to as "**Service Provider/ Vendor**", which expression shall mean to include its successors in title and permitted assigns of the Second Part:

WHEREAS

A. "The Bank" is carrying on business in banking in India and overseas and desirous to avail services for _____[3], and

   _____[4], and

B. Service Provider in the business of providing _____[5], and has agreed to supply _____ (Software) and/or providing the Services as mentioned in Request for Proposal (RFP) No. _____ dated _____issued by the Bank along with its clarifications/ corrigenda, referred hereinafter as a "RFP" and same shall be part of this Agreement.

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

1. DEFINITIONS & INTERPRETATION

[1]Name & Complete Address of the Dept.
[2]Name & Complete Address (REGISTERED OFFICE) of Service Provider,
[3]Purpose of the Agreement
[4]Any other connected purpose or details of RFP floated by the Bank
[5]Brief mentioning of service providers experience in providing the services required by the Bank.

1.1 Definition

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

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

1.1.2 "Code" shall mean computer programming code contained in the Software. If not otherwise specified, Code shall include both Object Code and Source Code which means programming languages, including all comments and procedural code, and all related development documents (e.g., flow charts, schematics, statements of principles of operations, end-user manuals, architecture standards, and any other specifications that are used to create or that comprise the Code). Code shall include Maintenance Modifications and Enhancements in the Software.

1.1.3 "Confidential Information" shall have the meaning set forth in Clause 15.

1.1.4 "Data Dictionary or Metadata Repository" shall mean a repository of information about data such as meaning, relationships to other data, origin/lineage, usage, business context and format including but not limited to data type, data length, data structure etc., further, it as a collection of columns and tables with metadata.

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

1.1.6 "Documentation" will describe in detail and in a completely self-contained manner how the user may access and use the Enterprise API Integration and Management Platform (name of the Software/ maintenance services),[6] such that any reader of the Documentation can access, use and maintain all of the functionalities of the Software, without the need for any further instructions. 'Documentation' includes, user manuals, installation manuals, operation manuals, design documents, process documents, data flow documents, data register, technical manuals, functional specification, software requirement specification, on-line tutorials/CBTs, system configuration documents, Data

[6] Name of Software

Dictionary, system/database administrative documents, debugging/diagnostics documents, test procedures, Review Records/ Test Bug Reports/ Root Cause Analysis Report, list of all Product components, list of all dependent/external modules and list of all documents relating to traceability of the Product as and when applicable etc.

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

1.1.8 "Open Source or Copyleft license" shall mean a license of a computer program in which the source code is available to the general public for use and/or modification from its original design.

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

1.1.10 "Project Documents" shall mean all the plans, drawings and specifications used while bidding and all other documents necessary to complete all work.

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

1.1.12 "Revision control procedure" shall mean the procedure for management of changes to documents, software programs, and other collections of information made during this engagement.

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

1.1.14 'Services' shall mean and include the Services offered by Service Provider more particularly described in Clause 2 of this Agreement. 'Services' shall also include the implementation services, training services and maintenance Services and other obligation of Service Provider to be provided under this Agreement.

1.1.15 "Software" shall mean (a) the software product(s) described in this Agreement; (b) all maintenance, modifications and enhancements that are provided to the

Bank; (c) the Code contained in or otherwise related to each of the foregoing; and (d) the Documentation.

1.1.16 "Test Bug Reports" shall mean a report providing the details as to the efficiency of software in relation with reporting and resolution of any bug.

1.1.17 **"Integrated Product Suite**": An **"***Integrated Product Suite***"** including below mentioned major components for deployment of the Enterprise API Integration and Management platform:

1. Enterprise Service Bus (ESB)
2. API Gateway
3. API Management and control
4. API Orchestration
5. API Security
6. Message Queuing Service
7. Integrated Product Monitoring

Note: "*Platform*" has been referred to as *"Integrated Product Suite"* in this SLA document.

1.1.18 "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.

1.1.19 **Enterprise API Integration and Management Platform** - The proposed integration platform - supply, installation, build, integration, designing, development, testing, operation, support and maintenance of which bids are invited. This will also be referred by "EIS 2.0".

1.1.20 **Resource Classification**: All resources for the entire duration of the Project will be classified in three categories L1, L2 and L3 as follows:

Table 3.1 Resource Category

Role / Resource Category	Experience	KRAs
Lead Architect, Team Manager, Project Manager, Program Manager, Product Manager, SMEs, Security expert, Network expert, ops/ Infra expert, Database Administrator, Database Developer, L3 etc. **(herein referred as L3)** <u>From OEM Only</u>	10+ Years	Understand needs and As-Is to define system design and specifications Communicate system requirements to development and QA teams; Act as the IT SPOC between SBI and SI/OEM team for the project Manage engineering and testing best practices; Drive API gateway adoption, ensuring adherence to standards, and coordinating efforts across stakeholders;

Senior Developer/ Designer, Senior Support Engineer, Sr. QA, Tech Lead, Team Lead, Senior Security resource, Senior Network resource, Senior ops/ Infra resource, L2 etc. **(herein referred as L2)** Not exceeding 30% by Channel Partner. Minimum 70% from OEM	6+ Years	Address advanced technical problems, perform in-depth diagnostics, and manage API lifecycle tasks such as version control and policy management. Ensure security enforcement, rate limiting, and orchestration, and provide detailed analytics; Program well-designed, testable, efficient code Execute full lifecycle feature development for Enterprise API Integration and Management Platform Document and maintain platform functionality etc.
Support engineer, Developer, QA tester, Security engineer, Network engineer, ops/ Infra engineer, L1 etc. **(herein referred as L1)** Can be from Channel Partner	3+ Years	Manage and troubleshoot platform and hosted APIs; Ensure audit and statutory compliance and perform patch installations. track bugs, Develop and execute automation scripts; Monitor platform performance and maintain documentation of recurring issues etc.

1.2 Interpretations:

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

1.2.2 The singular includes the plural and vice versa.

1.2.3 Reference to any gender includes each other gender.

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

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

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

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

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

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

1.3 Commencement, Term & Change in Terms

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

1.3.2 This Agreement shall be in force for a period of five (5) years from Effective Date, unless terminated by the Bank by notice in writing in accordance with the termination clauses of this Agreement.

1.3.3 The Bank shall have the right at its discretion to renew this Agreement in writing, for a further term of 2 years on the mutually agreed terms & conditions.

1.3.4 Either Party can propose changes to the scope, nature or time schedule of services being performed under this Service Level Agreement. Such changes can be made upon mutually accepted terms & conditions maintaining the spirit (Purpose) of this Service Level Agreement.

2. SCOPE OF WORK

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

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

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

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

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

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

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

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

3. FEES /COMPENSATION

3.1 Professional fees

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

3.1.2 _____

3.1.3 _____

3.2 All duties and taxes (excluding[7] Goods and Service Tax (GST) or any other tax imposed by the Government in lieu of same), if any, which may be levied, shall be borne by Service Provider and Bank shall not be liable for the same. All expenses, stamp duty and other charges/ expenses in connection with execution of this Agreement shall be borne by Service Provider. Goods and Service Tax (GST) or any other tax imposed by the Government in lieu of same shall be borne by the Bank on actual upon production of original receipt wherever required.

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

3.4 Payments

[7] Please determine the applicability of the taxes.

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

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

3.5 Bank Guarantee and Penalties

3.5.1 Service Provider shall furnish performance security in the form of Bank Guarantee for an amount of Rs. _____ valid for a period of __five_(5)__year(s) __three (3)__month(s) from a Scheduled Commercial Bank other than State Bank of India in a format provided/ approved by the Bank.

3.5.2 The Bank Guarantee is required to protect the interest of the Bank against delay in supply/installation and/or the risk of non-performance of Service Provider in respect of successful implementation of the project; or performance of the material or services sold; or breach of any terms and conditions of the Agreement, which may warrant invoking of Bank Guarantee.

3.5.3 If at any time during performance of the Contract, Service Provider shall encounter unexpected conditions impeding timely completion of the Services under the Agreement and performance of the services, Service Provider shall promptly notify the Bank in writing of the fact of the delay, it's likely duration and its cause(s). As soon as practicable, after receipt of Service Provider's notice, the Bank shall evaluate the situation and may at its discretion extend Service Provider's time for performance, in which case the extension shall be ratified by the Parties by amendment of the Agreement.

3.5.4 Performance of the obligations under the Agreement shall be made by Service Provider in accordance with the time schedule[8] specified in this Agreement.

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

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

3.5.6 Subject to Clause 17 of this Agreement, any unexcused delay by Service Provider in the performance of its Contract obligations shall render this Agreement to be terminated.

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

4. LIABILITIES/OBLIGATION

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

(i) Processing and authorising invoices

(ii) Approval of Information

(iii) _____

4.2 Service Provider Duties

(i) Service Delivery responsibilities

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

(b) Software solution provided and/or maintained by Service Provider shall be free from OWASP Top 10 vulnerabilities (latest) during the term of Agreement.

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

(d) Service Provider shall without any additional cost, rectify the vulnerabilities observed by the Bank during security review of Code. The Code shall be comprehensively reviewed periodically by the Bank or its authorized representative.

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

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

(g) Service Provider shall be responsible to provide Data Dictionary in a format provided by the Bank. During the term of this Agreement, such a format may be revised by the Bank as per the requirements. Service Provider shall capture all the fields in Data Dictionary format and keep the same always updated during the term of this Agreement.

(h) 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.

(i) The Service Provider shall execute Data Processing Agreement on the format attached as Appendix-Q to this RFP.

(j) 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.

(k) _____*<the concerned dept. may add duties depending on the nature of agreement>*

(ii) Security Responsibility

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

(b) _____

5. REPRESENTATIONS &WARRANTIES

5.1 Service Provider warrants that the technical quality and performance of the Services provided will be consistent with the mutually agreed standards. Warranty shall be for a period of 36 months (Term) from the date of acceptance.

5.2 Any defect found will be evaluated mutually to establish the exact cause of the defect. Bank may have direct and separate agreement with Service Provider to provide technical support to the Bank for related deficiencies.[9]

5.3 Service Provider warrants that at the time of delivery the Software or its component is free from malware, free from any obvious bugs, and free from any covert channels in the code (of the versions of the applications/software being delivered as well as any subsequent versions/modifications delivered).

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

5.5 Service Provider warrants that it shall be solely liable and responsible for compliance of applicable Labour Laws in respect of its employee, agents, representatives and sub-contractors (if allowed) and in particular laws relating to

[9]Please note the following clause can be kept only when there is a Separate Technical support agreement.

terminal benefits such as pension, gratuity, provident fund, bonus or other benefits to which they may be entitled and the laws relating to contract labour, minimum wages, etc., and the Bank shall have no liability in this regard.

5.6 Each Party represents and warrants that it has all requisite power and authorization to enter into and perform this Agreement and that nothing contained herein or required in the performance hereof conflict or will conflict with or give rise to a breach or default under, or permit any person or entity to terminate, any contract or instrument to which the party is bound.

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

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

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

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

5.11 Service Provider warrants that to the best of its knowledge, as on the Effective Date of this Agreement, the Software does not violate or infringe any patent, copyright, trademarks, trade secrets or other Intellectual Property Rights of any third party.

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

5.13 During the Warranty Period if any software or any component thereof is supplied by Service Provider is inoperable or suffers degraded performance not due to causes external to the software, Service provider shall, at the Bank's request, promptly replace the software or specified component with new software of the

same type and quality. Such replacement shall be accomplished without any adverse impact on the Bank's operations within agreed time frame.

5.14 _____<*any other additional warranty can be incorporated*>

6. GENERAL INDEMNITY

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

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

7. CONTINGENCY PLANS

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

8. TRANSITION REQUIREMENT

In the event of failure of Service Provider to render the Services or in the event of termination of Agreement or expiry of term or otherwise, without prejudice to any other right, the Bank at its sole discretion may make alternate arrangement for getting the Services contracted with another vendor. In such case, the Bank shall give prior notice to the existing Service Provider. The existing Service Provider shall continue to provide services as per the terms of the Agreement until a 'New Service Provider' completely takes over the work. During the transition phase, the existing Service Provider shall render all reasonable 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 vendor is breach of this obligation, they shall be liable for paying a penalty of 10% of the project cost on demand to the Bank, which may be settled from the payment of invoices or bank guarantee for the contracted period. Transition & Knowledge Transfer plan is mentioned in Annexure G.

9. LIQUIDATED DAMAGES

If Service Provider fails to deliver product and/or perform any or all the Services within the stipulated time, schedule as specified in this Agreement, the Bank may, without prejudice to its other remedies under the Agreement, and unless otherwise extension of time is agreed upon without the application of liquidated damages, deduct from the Project Cost, as liquidated damages a sum equivalent to 0.50 % of total Project cost for delay of each week or part thereof maximum up to 5.00 % of total Project cost. Once the maximum deduction is reached, the Bank may consider termination of the Agreement.

10. RELATIONSHIP BETWEEN THE PARTIES

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

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

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

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

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

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

11. SUB CONTRACTING

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

i. Sub-Contracting is not permitted. However, Bank may permit sub-contracting on case-to case basis at the sole discretion of the Bank. If permitted, the Service

Provider shall carry out its standard due diligence process on sub-contracting/ sub-contractor.

ii. Service Provider shall comply with all the instructions, requirements and any other conditions suggested by the Bank in order for the Bank to comply with its site access and regulatory audit requirements and upon' s Bank request Service Provider will provide a written confirmation of compliance with the requirements of this provision.

iii. With the Bank's prior written approval, Service Provider may change the sub-contractor, provided it does not impact the quality of Services being delivered. However, Service Provider shall inform the Bank on its intention to change the sub-contractor and reason thereof.

iv. Service Provider shall be responsible for all the Services provided to the Bank regardless of which entity is conducting the operations. Service Provider is also responsible for ensuring that the sub-contractor comply with all security/confidentiality requirements and other terms and conditions as applicable to Service Provider mentioned in this RFP. Bank reserves the right to conduct independent audit in this regard.

v. Service Provider shall ensure that suitable documents including confidentiality agreement are obtained from the sub-contractor and the Service Provider shall ensure that the secrecy and faith of the Bank's data / processes is maintained.

vi. Notwithstanding approval of the Bank for sub-contracting, the Service Provider shall remain liable to the Bank for all acts/omissions of sub-contractors.

vii. Service Provider shall ensure that it shall have all back-to-back commitments from its vendors in such agreements.

viii. Service Provider shall provide the complete details of Services sub-contracted by it including the details of sub-contractor(s) and/or its agent to the Bank as and when requested.

12. INTELLECTUAL PROPERTY RIGHTS

i. For any technology / Software / solution developed/used/supplied by Service Provider for performing Services or licensing and implementing Software and solution for the Bank as part of this RFP, Service Provider shall have right to use as well right to license for the outsourced services or third party 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 cost, 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 use of the technology / Software / products or any part thereof in India or abroad, for Software licensed/developed as part of this engagement. In case of violation/ infringement of patent/ trademark/ copyright/ trade secret or industrial design or any other Intellectual Property Right of third party, Service Provider shall, after due inspection and testing, without any additional cost (a) procure for the Bank the right to continue to using the Software supplied; or (b) replace or modify the Software to make it non-infringing so long as the replacement to or modification of Software provide substantially equivalent functional, performance and operational features as the infringing Software which is being replaced or modified; or (c) to the extent that the activities under clauses (a) and (b) above are not commercially reasonable, refund to the Bank all amounts paid by the Bank to Service Provider under this RFP/Agreement.

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

v. Service Provider shall have no obligations with respect to any infringement claims to the extent that the infringement claim arises or results from: (i) Service Provider's compliance with the Bank's specific technical designs or instructions (except where Service Provider knew or should have known that such compliance was likely to result in an infringement claim and Service Provider did not inform the Bank of the same); (ii) any unauthorized modification or alteration of the Software by the Bank or its employee; (iii) failure to implement an update to the licensed software that would have avoided the infringement, provided Service Provider has notified the Bank in writing that use of the update would have avoided the claim.

vi. Service Provider shall grant the Bank a fully paid-up, irrevocable, exclusive, unlimited, perpetual license throughout the territory of India or abroad to access,

replicate and use software provided by Service Provider, including all inventions, designs and marks embodied therein perpetually. The source code, object code, executable code and compilation procedures of the Software Solution over and above the OEM products, made under this agreement, are the proprietary property of the Bank and as such Service Provider shall make them available to the Bank after successful User Acceptance Testing. 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. This also includes architecture design, network design, infrastructure design, integration design etc. implemented at SBI. Any work made under this agreement shall be deemed to be 'work made for hire' under any Indian/U.S. or any other applicable copyright laws.

13. INSTALLATION

Service provider will install the software/support the Bank in installation of the software developed into the Bank's production, disaster recovery, testing and training environment, if required.

14. INSPECTION AND AUDIT

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

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

auditors covering the respective risk parameters against which such Deficiencies observed.

14.3 Service Provider further agrees that whenever required by the Bank, it will furnish all relevant information, records/data to such auditors and/or inspecting officials of the Bank/ Reserve Bank of India and/or any regulatory authority (ies). The Bank reserves the right to call for and/or retain any relevant information/ audit reports on financial and security 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 break-ups etc.).

14.4 Service Provider shall grants unrestricted and effective access to a) data related to the Services; b) the relevant business premises of the Service Provider; subject to appropriate security protocols, for the purpose of effective oversight use by the Bank, their auditors, regulators and other relevant Competent Authorities, as authorised under law.

15. CONFIDENTIALITY

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

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

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

15.4 Each party agrees that it will not disclose any Confidential Information received from the other to any third parties under any circumstances without the prior written consent of the other party unless such disclosure of Confidential Information is required by law, legal process or any order of any government authority. Service provider, in this connection, agrees to abide by the laws especially applicable to confidentiality of information relating to customers of Banks and the banks per-se, even when the disclosure is required under the law. In such event, the Party must notify the other Party that such disclosure has been made in accordance with law; legal process or order of a government authority.

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

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

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

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

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

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

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

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

15.8 Receiving party undertakes to promptly notify disclosing party in writing any breach of obligation of the Agreement by its employees or representatives including confidentiality obligations. Receiving party acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that disclosing party

shall be entitled, without waiving any other rights or remedies, to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.

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

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

15.11 Upon expiration or termination of the Agreement, all the Bank's proprietary documents, customized programs partially or wholly completed and associated documentation, or the Bank's materials which are directly related to any project under the Agreement shall be delivered to the Bank or at the Bank's written instruction destroyed, and no copies shall be retained Service provider without the Bank's written consent.

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

16. OWNERSHIP

16.1 Service Provider will provide Source Code for every version of the Software supplied or customized/developed specifically for the Bank, without any cost to the Bank, and it will be treated as the property of the Bank.

16.2 The Source Code /Object Code /executable code and compilation procedures of the Software solution made under this Agreement are the proprietary property of the Bank and as such Service provider shall make them available to the Bank after successful User Acceptance Testing.

16.3 Service Provider agrees that the Bank owns the entire right, title and interest to any inventions, designs, discoveries, writings and works of authorship, including all Intellectual Property Rights, copyrights. Any work made under this Agreement shall be deemed to be 'work made for hire' under any Indian/U.S. or any other applicable copyright laws.

16.4 Service Provider shall ensure proper change management process covering impact assessment, requirement and solution documents detailing changes made to the Software for any work order, in addition to enabling the programmers identify and track the changes made to the source code. The Source Code will be delivered in appropriate version control tool maintained at the Bank's on site location.

16.5 Service Provider shall adhere to revision control procedure of the Bank to maintain required documentation and configuration files as well as Source Code.

Necessary backup and restoration of the revision control software related information will be handled by the service team as per the approved backup policy of the Bank.

16.6 For each application developed by Service Provider on Software, including third party software before the platform become operational, Service Provider shall deliver all documents to the Bank, which include coding standards, user manuals, installation manuals, operation manuals, design documents, process documents, technical manuals, and other documents, if any, as per work order.

16.7 Service Provider shall also provide documents related to Review Records/ Test Bug Reports/ Root Cause Analysis Report, details and documentation of all product components, details and documentation of all dependent/ external modules and all documents relating to traceability of the Software supplied/ customized under this Agreement before its production release.

16.8 All Software programs supplied/developed, program documentation, system documentation and testing methodologies along with all other information and documents (other than tools being proprietary to Service Provider) and used for customized Software development shall be the exclusive property of the Bank.

16.9 The Intellectual Property Rights on the Software Code, copyright and source code for various applications/ interfaces developed under this Agreement, and any other component/ framework/ middleware used/ developed as pre-built software assets to deliver the solution, shall belong to the Bank and the Bank shall have complete and unrestricted rights on such property. However, Service Provider shall hold All Intellectual Property rights in any pre-built software *per se*, except for those which have been assigned under this Agreement.

16.10 All information processed by Service Provider during Software development/ customization, implementation& 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.

17. Intentionally left blank

18. TERMINATION

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

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

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

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

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

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

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

18.3 In the event the bank terminates the Agreement in whole or in part for the breaches attributable to Service Provider, the Bank may procure, upon such terms and in such manner, as it deems appropriate, software or services similar to those undelivered and subject to clause 21 Service Provider shall be liable to the Bank for any excess costs for such similar software or services. However, Service provider, in case of part termination, shall continue the performance of the Agreement to the extent not terminated.

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

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

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

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

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

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

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

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

19. DISPUTE REDRESSAL MACHANISM & GOVERNING LAW

19.1 All disputes or differences whatsoever arising between the parties out of or in connection with this Agreement, if any, or in discharge of any obligation arising out of this Agreement and the Contract (whether during the progress of work or after completion of such work and whether before or after the termination of the contract, abandonment or breach of the contract), shall be settled amicably. If however, the parties are not able to solve them amicably within 30 (Thirty) days after the dispute occurs, as evidenced through the first written communication from any Party notifying the other regarding the disputes, the same shall be referred to and be subject to the jurisdiction of competent Civil Courts of Mumbai only. The Civil Courts in Mumbai, Maharashtra shall have exclusive jurisdiction in this regard.

19.2 Service Provider shall continue work under the Contract during the dispute resolution proceedings unless otherwise directed by the Bank or unless the matter is such that the work cannot possibly be continued until the decision of the competent court is obtained.

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

20. POWERS TO VARY OR OMIT WORK

20.1 No alterations, amendments, omissions, additions, suspensions or variations of the work (hereinafter referred to as variation) under the Agreement shall be made by Service provider except as directed in writing by Bank. The Bank shall have full powers, subject to the provision herein after contained, from time to time during the execution of the Agreement, by notice in writing to instruct Service Provider to make any variation without prejudice to the Agreement. Service Provider shall carry out such variations and be bound by the same conditions, though the said variations occurred in the Agreement documents. If any suggested variations would, in the opinion of Service Provider, if carried out, prevent them from fulfilling any of their obligations under the Agreement, they

shall notify the Bank, thereof, in writing with reasons for holding such opinion and Bank shall instruct Service Provider to make such other modified variation without prejudice to the Agreement. Service Provider shall carry out such variations and be bound by the same conditions, though the said variations occurred in the Agreement documents. If Bank confirms their instructions Service Provider's obligations will be modified to such an extent as may be mutually agreed. If such variation involves extra cost, any agreed difference in cost occasioned by such variation shall be mutually agreed between the parties. In any case in which Service Provider has received instructions from the Bank as to the requirement of carrying out the altered or additional substituted work, which either then or later on, will in the opinion of Service Provider, involve a claim for additional payments, such additional payments shall be mutually agreed in line with the terms and conditions of the order.

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

21. WAIVER OF RIGHTS

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

22. LIMITATION OF LIABILITY

22.1 The maximum aggregate liability of Service Provider, subject to below mentioned sub-clause 21.3, in respect of any claims, losses, costs or damages arising out of or in connection with this Agreement shall not exceed the total Project Cost.

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

22.3 The limitations set forth in abovementioned sub-Clause 21.1 shall not apply with respect to:

(i) claims that are the subject of indemnification pursuant to Clause 12[10] (infringement of third party Intellectual Property Right);

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

[10] Please see Clause 12 'IPR Indemnification'

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

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

For the purpose of above mentioned sub-clause 21.3(ii) "Gross Negligence" means any act or failure to act by a party which was in reckless disregard of or gross indifference to the obligation of the party under this Agreement and which causes injury, damage to life, personal safety, real property, harmful consequences to the other party, which such party knew, or would have known if it was acting as a reasonable person, would result from such act or failure to act for which such Party is legally liable. Notwithstanding the forgoing, Gross Negligence shall not include any action taken in good faith.

"Willful Misconduct" means any act or failure to act with an intentional disregard of any provision of this Agreement, which a party knew or should have known if it was acting as a reasonable person, which would result in injury, damage to life, personal safety, real property, harmful consequences to the other party, but shall not include any error of judgment or mistake made in good faith.

23. FORCE MAJEURE

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

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

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

23.4 If the Force Majeure situation continues beyond 30 (thirty) days, either Party shall have the right to terminate the Agreement by giving a notice to the other Party. Neither Party shall have any penal liability to the other in respect of the termination of this Agreement as a result of an event of Force Majeure. However,

Service Provider shall be entitled to receive payments for all services actually rendered up to the date of the termination of this Agreement.

24. NOTICES

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

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

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

(a) In the case of the Bank

DGM (IT-EIS 2.0)
State Bank of India Global IT Centre, C
BD Belapur, Sector-11, Navi Mumbai- 400614

(b) In case of Service Provider

_____
_____
_____

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

25. GENERAL TERMS & CONDITIONS

25.1 TRAINING: Service Provider shall train designated Bank officials on the configuration, operation/ functionalities, maintenance, support & administration for Software, application architecture and components, installation, troubleshooting processes of the proposed Services as mentioned in this Agreement.

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

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

25.4 NON-HIRE AND NON-SOLICITATION: During the term of this Agreement and for a period of one year thereafter, neither Party shall (either directly or indirectly through a third party) employ, solicit to employ, cause to be solicited for the purpose of employment or offer employment to any employee(s) of the

other Party, or aid any third person to do so, without the specific written consent of the other Party. However, nothing in this clause shall affect the Bank's regular recruitments as per its recruitment policy and not targeted to the employees of Service provider.

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

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

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

(i) This Agreement;
(ii) Annexure of Agreement;
(iii) Purchase Order No._____ dated _____; and
(iv) RFP

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

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

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

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

State Bank of India	**_____Service Provider**
By:	**By:**
Name:	**Name:**
Designation:	**Designation:**
Date:	**Date:**

WITNESS:

1. 1.

2. 2.

ANNEXURE-A

DELIVERABLES/SCOPE OF WORK

As detailed in RFP (Appendix E)

ANNEXURE-B

INFRASTUCTURE MANAGEMENT METRICS

As detailed in RFP (Appendix E and Appendix J of the RFP)

ANNEXURE-C

APPLICATION DEVELOPMENT & MAINTENANCE METRIC.

As detailed in RFP (Appendix E)

ANNEXURE-D

SERVICE DESK SUPPORT METRIC

As detailed in RFP (Appendix E)

SERVICE LEVEL REPORTING/ FREQUENCY

As detailed in RFP (Appendix E)

ANNEXURE-E

ESCALATION MATRICS[11]

Service level Category	Response/Resolution Time	Escalation thresholds			
		Escalation Level 1		Escalation.....	
		Escalation to	Escalation Mode	Escalation to	Escalation Mode
Production Support		*<Name, designation contact no.>*			
Service Milestones		*<Name, designation contact no.>*			
Infrastructure Management		*<Name, designation contact no.>*			
Application Development & Maintenance		*<Name, designation contact no.>*			
Information Security		*<Name, designation contact no.>*			
Service Desk Support		*<Name, designation contact no.>*			

[11] To ensure that the service beneficiary receives senior management attention on unresolved issues, Service Provider operates a problem escalation procedure in order that any unresolved problems are notified to Service Provider management personnel on a priority basis dependent upon the impact and urgency of the problem.

ANNEXURE-F

PENALTY FOR NON PERFORMANCE OF SLA

As detailed in RFP (Appendix J)

ANNEXURE G

Transition & Knowledge Transfer Plan

1. Introduction

This Annexure describes the duties and responsibilities of Service Provider and the Bank to ensure proper transition of services and to ensure complete knowledge transfer.

2. Objectives

The objectives of this annexure are to:

(1) ensure a smooth transition of Services from Service Provider to a New/Replacement SERVICE PROVIDER or back to the Bank at the termination or expiry of this Agreement;

(2) ensure that the responsibilities of both parties to this Agreement are clearly defined in the event of exit and transfer; and

(3) ensure that all relevant Assets are transferred.

3. General

3.1 Where the Bank intends to continue equivalent or substantially similar services to the Services provided by Service Provider after termination or expiry the Agreement, either by performing them itself or by means of a New/Replacement SERVICE PROVIDER, Service Provider shall ensure the smooth transition to the Replacement SERVICE PROVIDER and shall co-operate with the Bank or the Replacement SERVICE PROVIDER as required in order to fulfil the obligations under this annexure.

3.2 Service Provider shall co-operate fully with the Bank and any potential Replacement SERVICE PROVIDERs tendering for any Services, including the transfer of responsibility for the provision of the Services previously performed by Service Provider to be achieved with the minimum of disruption. In particular:

3.2.1 during any procurement process initiated by the Bank and in anticipation of the expiry or termination of the Agreement and irrespective of the identity of any potential or actual Replacement SERVICE PROVIDER, Service Provider shall comply with all reasonable requests by the Bank to provide information relating to the operation of the Services, including but not limited to, hardware and software used, inter-working, coordinating with other application owners, access to and provision of all performance reports, agreed procedures, and any other relevant information (including the configurations set up for the Bank and procedures used by Service Provider for handling Data) reasonably necessary to achieve an effective transition, provided that:

3.2.1.1 Service Provider shall not be obliged to provide any information concerning the costs of delivery of the Services or any part thereof or disclose the financial records of Service Provider to any such party;

3.2.1.2 Service Provider shall not be obliged to disclose any such information for use by an actual or potential Replacement SERVICE PROVIDER unless such a party shall have entered into a confidentiality agreement; and

3.2.1.3 whilst supplying information as contemplated in this paragraph 3.2.1 Service Provider shall provide sufficient information to comply with the reasonable requests of the Bank to enable an effective tendering process to take place but shall not be required to provide information or material which Service Provider may not disclose as a matter of law.

3.3 In assisting the Bank and/or the Replacement SERVICE PROVIDER to transfer the Services the following commercial approach shall apply:

(1) where Service Provider does not have to utilise resources in addition to those normally used to deliver the Services prior to termination or expiry, Service Provider shall make no additional Charges. The Bank may reasonably request that support and materials already in place to provide the Services may be redeployed onto work required to effect the transition provided always that where the Bank agrees in advance that such redeployment will prevent Service Provider from meeting any Service Levels, achieving any other key dates or from providing any specific deliverables to the Bank, the Bank shall not be entitled to claim any penalty or liquidated damages for the same.

(2) where any support and materials necessary to undertake the transfer work or any costs incurred by Service Provider are additional to those in place as part of the proper provision of the Services the Bank shall pay Service Provider for staff time agreed in advance at the rates agreed between the parties and for materials and other costs at a reasonable price which shall be agreed with the Bank.

3.4 If so required by the Bank, on the provision of no less than 15 (fifteen) days' notice in writing, Service Provider shall continue to provide the Services or an agreed part of the Services for a period not exceeding **6 (Six)** months beyond the date of termination or expiry of the Agreement. In such event the Bank shall reimburse Service Provider for such elements of the Services as are provided beyond the date of termination or expiry date of the Agreement on the basis that:

(1) Services for which rates already specified in the Agreement shall be provided on such rates;

(2) materials and other costs, if any, will be charged at a reasonable price which shall be mutually agreed between the Parties.

3.5 Service Provider shall provide to the Bank an analysis of the Services to the extent reasonably necessary to enable the Bank to plan migration of such workload to a Replacement SERVICE PROVIDER provided always that this analysis involves providing performance data already delivered to the Bank as part of the performance monitoring regime.

3.6 Service Provider shall provide such information as the Bank reasonably considers to be necessary for the actual Replacement SERVICE PROVIDER, or any potential

Replacement SERVICE PROVIDER during any procurement process, to define the tasks which would need to be undertaken in order to ensure the smooth transition of all or any part of the Services.

3.7 Service Provider shall make available such Key Personnel who have been involved in the provision of the Services as the Parties may agree to assist the Bank or a Replacement SERVICE PROVIDER (as appropriate) in the continued support of the Services beyond the expiry or termination of the Agreement, in which event the Bank shall pay for the services of such Key Personnel on a time and materials basis at the rates agreed between the parties.

3.8 Service Provider shall co-operate with the Bank during the handover to a Replacement SERVICE PROVIDER and such co-operation shall extend to, but shall not be limited to, inter-working, co-ordinating and access to and provision of all operational and performance documents, reports, summaries produced by Service Provider for the Bank, including the configurations set up for the Bank and any and all information to be provided by Service Provider to the Bank under any other term of this Agreement necessary to achieve an effective transition without disruption to routine operational requirements.

4. Replacement SERVICE PROVIDER

In the event that the Services are to be transferred to a Replacement SERVICE PROVIDER, the Bank will use reasonable endeavors to ensure that the Replacement SERVICE PROVIDER co-operates with Service Provider during the handover of the Services.

5. Subcontractors

Service Provider agrees to provide the Bank with details of the Subcontracts (if permitted by the Bank) used in the provision of the Services. Service Provider will not restrain or hinder its Subcontractors from entering into agreements with other prospective service providers for the delivery of supplies or services to the Replacement SERVICE PROVIDER.

6. Transfer of Configuration Management Database

6 (six) months prior to expiry or within 2 (two) week of notice of termination of this Agreement Service Provider shall deliver to the Bank a full, accurate and up to date cut of content from the Configuration Management Database (or equivalent) used to store details of Configurable Items and Configuration Management data for all products used to support delivery of the Services.

7. Transfer of Assets

7.1 6 (six) months prior to expiry or within2 (two) week of notice of termination of the Agreement Service Provider shall deliver to the Bank the Asset Register comprising:

(1) a list of all Assets eligible for transfer to the Bank; and

(2) a list identifying all other Assets, (including human resources, skillset requirement and know-how), that are ineligible for transfer but which are essential to the delivery of the Services. The purpose of each component and the reason for ineligibility for transfer shall be included in the list.

7.2 Within 1 (one) month of receiving the Asset Register as described above, the Bank shall notify Service Provider of the Assets it requires to be transferred, (the "Required Assets"), and the Bank and Service Provider shall provide for the approval of the Bank a draft plan for the Asset transfer.

7.3 In the event that the Required Assets are not located on Bank premises:

(1) Service Provider shall be responsible for the dismantling and packing of the Required Assets and to ensure their availability for collection by the Bank or its authorised representative by the date agreed for this;

(2) any charges levied by Service Provider for the Required Assets not owned by the Bank shall be fair and reasonable in relation to the condition of the Assets and the then fair market value; and

(3) for the avoidance of doubt, the Bank will not be responsible for the Assets.

7.4 Service Provider warrants that the Required Assets and any components thereof transferred to the Bank or Replacement SERVICE PROVIDER benefit from any remaining manufacturer's warranty relating to the Required Assets at that time, always provided such warranties are transferable to a third party.

8. Transfer of Software Licenses

8.1 6 (six) months prior to expiry or within 2 (two) week of notice of termination of this Agreement Service Provider shall deliver to the Bank all licenses for Software used in the provision of Services which were purchased by the Bank.

8.2 On notice of termination of this Agreement Service Provider shall, within 2 (two) week of such notice, deliver to the Bank details of all licenses for SERVICE PROVIDER Software and SERVICE PROVIDER Third Party Software used in the provision of the Services, including the terms of the software license agreements. For the avoidance of doubt, the Bank shall be responsible for any costs incurred in the transfer of licenses from Service Provider to the Bank or to a Replacement SERVICE PROVIDER provided such costs shall be agreed in advance. Where transfer is not possible or not economically viable the Parties will discuss alternative licensing arrangements.

8.3 Within 1 (one)month of receiving the software license information as described above, the Bank shall notify Service Provider of the licenses it wishes to be transferred, and Service Provider shall provide for the approval of the Bank a draft plan for license transfer, covering novation of agreements with relevant software providers, as required. Where novation is not possible or not economically viable the Parties will discuss alternative licensing arrangements.

9. Transfer of Software

Wherein State Bank of India is the owner of the software, 6 (six) months prior to expiry or within 2 (two) weeks of notice of termination of this Agreement Service Provider shall deliver, or otherwise certify in writing that it has delivered, to the Bank a full, accurate and up to date version of the Software including up to date versions and latest releases of, but not limited to:

(a) Source Code (with source tree) and associated documentation;
(b) application architecture documentation and diagrams;
(c) release documentation for functional, technical and interface specifications;
(d) a plan with allocated resources to handover code and design to new development and test teams (this should include architectural design and code 'walk-through');
(e) Source Code and supporting documentation for testing framework tool and performance tool;
(f) test director database;
(g) test results for the latest full runs of the testing framework tool and performance tool on each environment; and

10. Transfer of Documentation

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

11. Transfer of Service Management Process

6 (six) months prior to expiry or within 2 (two) weeks of notice of termination of this Agreement Service Provider shall deliver to the Bank:

(a) a plan for the handover and continuous delivery of the Service Desk function and allocate the required resources;
(b) full and up to date, both historical and outstanding Service Desk ticket data including, but not limited to:
    (1) Incidents;
    (2) Problems;
    (3) Service Requests;
    (4) Changes;
    (5) Service Level reporting data;
(c) a list and topology of all tools and products associated with the provision of the Software and the Services;
(d) full content of software builds and server configuration details for software deployment and management; and
(e) monitoring software tools and configuration.

12. Transfer of Knowledge Base

6 (six) months prior to expiry or within 2 (two) week of notice of termination of this Agreement Service Provider shall deliver to the Bank a full, accurate and up to date cut of content from the knowledge base (or equivalent) used to troubleshoot issues arising with the Services but shall not be required to provide information or material which Service Provider may not disclose as a matter of law.

13. Transfer of Service Structure

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

(a) archive of records including:
  (1) Questionnaire Packs;
  (2) project plans and sign off;
  (3) Acceptance Criteria; and
  (4) Post Implementation Reviews.

(b) programme plan of all work in progress currently accepted and those in progress;

(c) latest version of documentation set;

(d) Source Code (if appropriate) and all documentation to support the services build tool with any documentation for 'workarounds' that have taken place;

(e) Source Code, application architecture documentation/diagram and other documentation;

(f) Source Code, application architecture documentation/diagram and other documentation for Helpdesk; and

(g) project plan and resource required to hand Service Structure capability over to the new team.

14. Transfer of Data

14.1 In the event of expiry or termination of this Agreement Service Provider shall cease to use the Bank's Data and, at the request of the Bank, shall destroy all such copies of the Bank's Data then in its possession to the extent specified by the Bank.

14.2 Except where, pursuant to paragraph 14.1 above, the Bank has instructed Service Provider to destroy such Bank's Data as is held and controlled by Service Provider, 1 (one) months prior to expiry or within 1 (one) month of termination of this Agreement, Service Provider shall deliver to the Bank:

(1) An inventory of the Bank's Data held and controlled by Service Provider, plus any other data required to support the Services; and/or

(2) a draft plan for the transfer of the Bank's Data held and controlled by Service Provider and any other available data to be transferred.

15. Training Services on Transfer

15.1 Service Provider shall comply with the Bank's reasonable request to assist in the identification and specification of any training requirements following expiry or termination. The purpose of such training shall be to enable the Bank or a Replacement SERVICE PROVIDER to adopt, integrate and utilize the Data and Assets transferred and to deliver an equivalent service to that previously provided by Service Provider.

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

15.3 Subject to paragraph 15.2 above, Service Provider shall produce for the Bank's consideration and approval 6 (six) months prior to expiry or within 10 (ten) working days of issue of notice of termination:

(1) A training strategy, which details the required courses and their objectives;

(2) Training materials (including assessment criteria); and

(3) a training plan of the required training events.

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

15.5 SERVICE PROVIDER shall provide training courses on operation of licensed /open source software product at Bank's _____Premises, at such times, during business hours as Bank may reasonably request. Each training course will last for _____hours. Bank may enroll up to _____ of its staff or _____ employees of the new/replacement service provider in any training course, and Service Provider shall provide a hard copy of the Product (licensed or open sourced) standard training manual for each enrollee. Each training course will be taught by a technical expert with no fewer than _____ years of experience in operating _____software system. SERVICE PROVIDER shall provide the _____ training without any additional charges.

16. Transfer Support Activities

16.1 6 (six) months prior to expiry or within 10 (ten) Working Days of issue of notice of termination, Service Provider shall assist the Bank or Replacement SERVICE PROVIDER to develop a viable exit transition plan which shall contain details of the tasks and responsibilities required to enable the transition from the Services provided under this Agreement to the Replacement SERVICE PROVIDER or the Bank, as the case may be.

16.2 The exit transition plan shall be in a format to be agreed with the Bank and shall include, but not be limited to:

(1) a timetable of events;

(2) resources;

(3) assumptions;

(4) activities;

(5) responsibilities; and

(6) risks.

16.3 Service Provider shall supply to the Bank or a Replacement SERVICE PROVIDER specific materials including but not limited to:

(a) Change Request log;

(b) entire back-up history; and

(c) dump of database contents including the Asset Register, problem management system and operating procedures. For the avoidance of doubt this shall not include proprietary software tools of Service Provider which are used for project management purposes generally within Service Provider's business.

16.4 Service Provider shall supply to the Bank or a Replacement SERVICE PROVIDER proposals for the retention of Key Personnel for the duration of the transition period.

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

16.6 Service Provider shall provide to the Bank or to any Replacement SERVICE PROVIDER within 14 (fourteen) Working Days of expiry or termination a full and complete copy of the Incident log book and all associated documentation recorded by Service Provider till the date of expiry or termination.

16.7 Service Provider shall provide for the approval of the Bank a draft plan to transfer or complete work-in-progress at the date of expiry or termination.

17. Use of Bank Premises

17.1 Prior to expiry or on notice of termination of this Agreement, Service Provider shall provide for the approval of the Bank a draft plan specifying the necessary steps to be taken by both Service Provider and the Bank to ensure that the Bank's Premises are vacated by Service Provider.

17.2 Unless otherwise agreed, Service Provider shall be responsible for all costs associated with Service Provider's vacation of the Bank's Premises, removal of equipment and furnishings, redeployment of SERVICE PROVIDER Personnel, termination of arrangements with Subcontractors and service contractors and restoration of the Bank Premises to their original condition (subject to a reasonable allowance for wear and tear).

XXXXX

ANNEXURE-H

Data Processing Agreement

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

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

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

And

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

WHEREAS:

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

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

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

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

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation:

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

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

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

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

1.1.4 "Data Protection Legislation" means as applicable, the UK Data Protection Act 1998, Directive 95/46/EC of the European Parliament and any laws or regulations implementing

it, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and any equivalent or replacement law in the UK and any other data protection and privacy laws applicable to the Services.

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

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

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

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

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

1.1.10 "EEA" means the European Economic Area.

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

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

1.1.13 "Data Transfer" means:

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

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

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

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

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

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

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

2. Processing of Personal Data:

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

2.2 Processor shall:

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

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

3. PROCESSOR OBLIGATIONS:

3.1 Processor Personnel:

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

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

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

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

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

3.2 Security:

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

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

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

3.3 Sub-Processing:

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

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

3.4 Data Subject Rights:

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

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

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

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

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

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

3.5 Personal Data Breach:

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

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

3.6 Data Protection Impact Assessment and Prior Consultation:

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

3.7 Deletion or return of Personal Data:

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

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

3.8 Audit Rights:

The Processor shall make available to State Bank of India and any supervisory authority or their representatives the information necessary to demonstrate its compliance with this Agreement and allow for and contribute to audits and inspections by allowing State Bank of India, its Client, a supervisory authority or their representatives to conduct an audit or inspection of that part of the Processor's business which is relevant to the Services [on at

least an annual basis (or more frequently when mandated by a relevant supervisory authority or to comply with the Data Protection Legislation) and] on reasonable notice, in relation to the Processing of Personal Data by the Processor.

3.9 Data Transfer:

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

3.10 Records:

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

3.11 Notify:

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

3.12 Agreement Termination:

Upon expiry or termination of this Agreement or the Services for any reason or State Bank of India's earlier request, the Procesor 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:
5.3.1This 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		
		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		a. Web		

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

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

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

S. No	Controls to be implemented		Compliance (Yes / No)	If under implementation, give date by which implementation will be done
		f. No Sharing of data with any third party without explicit written permission from competent Information Owner of the Bank including the Law Enforcement Agencies.		

_____XXXXX_____

ANNEXURE-H

Data Processing Agreement

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

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

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

And

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

WHEREAS:

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

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

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

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

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation:

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

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

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

1.1.3 “Client” means a customer of State Bank of India.

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

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

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

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

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

1.1.9 "Data Protection Laws" means EU Data Protection Laws and, to the extent

applicable, the data protection or privacy laws of any other country.

1.1.10 "EEA" means the European Economic Area.

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

supplementing the GDPR.

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

1.1.13 "Data Transfer" means:

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

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

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

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

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

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

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

2. Processing of Personal Data:

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

2.2 Processor shall:

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

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

3. PROCESSOR OBLIGATIONS:

3.1 Processor Personnel:

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

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

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

3.1.3. The Processor shall immediately notify State Bank of India if, in Processor's

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

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

3.2 Security:

3.2.1 Taking into account the nature, scope, context and purposes of Processing

(provided in Schedule 2) as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to Personal Data implement appropriate technical and organizational measures (Processor obligations in Schedule 3) to

ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

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

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

3.3 Sub-Processing:

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

3.3.2 The Processor shall include in any contract with its Sub processors who will

process Personal Data on State Bank of India's behalf, obligations on such Sub processors which are no less onerous than those obligations imposed upon the

Processor in this Agreement relating to Personal Data. The Processor shall be liable for the acts and omissions of its Sub processors to the same extent to which the Processor would be liable if performing the services of each Sub processor directly under the terms of this Agreement.

3.4 Data Subject Rights:

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

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

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

3.4.2.1 promptly notify SBI if it receives a request from a Data Subject under

any Data Protection Law in respect of Personal Data; and

3.4.2.2 ensure that it does not respond to that request except on the

documented instructions of SBI or as required by Applicable Laws to

which the Processor is subject, in which case Processor shall to the

extent permitted by Applicable Laws

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

the request.

3.5 Personal Data Breach:

3.5.1 Processor shall notify SBI without undue delay upon Processor becoming aware of a Personal Data Breach affecting Personal Data, providing SBI with sufficient information to

allow SBI to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

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

3.6 Data Protection Impact Assessment and Prior Consultation:

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

3.7 Deletion or return of Personal Data:

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

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

3.8 Audit Rights:

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

or to comply with the Data Protection Legislation) and] on reasonable notice, in relation to the Processing of Personal Data by the Processor.

3.9 Data Transfer:

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

3.10 Records:

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

3.11 Notify:

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

3.12 Agreement Termination:

Upon expiry or termination of this Agreement or the Services for any reason or State Bank of India's earlier request, the Procesor 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:

5.3.1This 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:	Business Continuity Management		
		Backup management		
		Desktop/system/server/network device hardening with baseline controls		
		Patch Management		
		Port Management Media Movement		
		Log Management		
		Personnel Security		
		Physical Security		
		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	Firewall		
		WAF		

	environment is suitably protected from external threats by way of:	IDS/IPS		
		AD		
		AV		
		NAC		
		DLP		
		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:	Web		
		Application		
		DB		
		Configuration		
		User access		
10	Whether the Processor maintains logs for privileged access to their critical systems?			
11	Whether privilege access to the Processor environment is permitted from internet?			
12	Whether the Processor has captive SOC or Managed Service SOC for monitoring their systems and operations?			
13	Whether the Processor environment is segregated into militarized zone (MZ) and demilitarized zone (DMZ) separated by Firewall, where any access from an external entity is permitted through DMZ only?			
14	Whether Processor has deployed secure environments for their applications for:	Production		
		Disaster recovery		
		Testing environments		
15	Whether the Processor follows the best practices of creation of	Web		
		App		
		DB		
		Critical applications		

	separate network zones (VLAN Segments) for:	Non-Critical applications		
		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:	Internal servers		
		Database servers		
		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?			
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.			
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:	Right to Audit to SBI with scope defined		
		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.		
		Right to recall data by SBI.		
		Regulatory and Statutory compliance at vendor site. Special emphasis on section 43A of IT Act 2000 apart from others.		
		Availability of Compensation clause in case of any data breach or incident resulting into any type of loss to SBI, due to vendor negligence.		

		No Sharing of data with any third party without explicit written permission from competent Information Owner of the Bank including the Law Enforcement Agencies.		

_____XXXXX_____

[1]Name & Complete Address of the Dept.
[2]Name & Complete Address (REGISTERED OFFICE) of Service Provider,
[3]Purpose of the Agreement
[4]Any other connected purpose or details of RFP floated by the Bank
[5]Brief mentioning of service providers experience in providing the services required by the Bank.
[6] Name of Software
[7] Please determine the applicability of the taxes.
[8] Please ensure that the time scheduled is suitably incorporated in the Agreement.
[9]Please note the following clause can be kept only when there is a Separate Technical support agreement.
[10] Please see Clause 12 'IPR Indemnification'
[11] To ensure that the service beneficiary receives senior management attention on unresolved issues, Service Provider operates a problem escalation procedure in order that any unresolved problems are notified to Service Provider management personnel on a priority basis dependent upon the impact and urgency of the problem.

Appendix-L

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:**

1.1 "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

1.2 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.

1.3 "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**

2.1 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 the Service Provider appoints any Sub-Contractor (if allowed) then the 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.

2.2 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

iii. government or regulatory authorities regulating the affairs of the parties and inspectors and supervisory bodies thereof

2.3 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**

3.1 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.

3.2 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.

3.3 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.

a. Suspension of access privileges
b. Change of personnel assigned to the job
c. Termination of contract

3.4 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**

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

4.7 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.

4.8 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.

4.9 The Agreement shall be effective from _____ ("Effective Date") and shall be valid for a period of _____ year(s) thereafter (the "Agreement Term"). The foregoing obligations as to confidentiality shall survive the term of this Agreement and for a period of five (5) years thereafter provided confidentiality obligations with respect to individually identifiable information, customer's data of Parties or software in human-readable form (e.g., source code) shall survive in perpetuity.

5. **Suggestions and Feedback**

Either party from time to time may provide suggestions, comments or other feedback to the other party with respect to Confidential Information provided originally by the other party (hereinafter "feedback"). Both party agree that all Feedback is and shall be entirely voluntary and shall not in absence of separate agreement, create any confidentially obligation for the receiving party. However, the Receiving Party shall not disclose the source of any feedback without the providing party's consent. Feedback shall be clearly designated as such and, except as otherwise provided herein, each party shall be free to disclose and use such Feedback as it sees fit, entirely without obligation of any kind to other party. The foregoing shall not, however, affect either party's obligations hereunder with respect to Confidential Information of other party.

Dated this _____ day of _____ (Month) *20*__ at _____(place)

For and on behalf of _____

Name		
Designation		
Place		
Signature		

For and on behalf of _____

Name		
Designation		
Place		
Signature		

Appendix-M

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

To be provided in excel format

Appendix-N

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	
Project Deliverables (description in brief)	
Products used in the Project with regards to "Integrated Product Suite"	
Start Date	
End Date	
Current Status (In Progress / Completed)	
Size of Project	
Value of Work Order (In Lakh) (only single work order)	

Please Note: All the fields are Mandatory Fields

Name & Signature of authorised signatory

Seal of Company

Appendix-O

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 :

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

- Enabling BIDDERs to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also

abstain from bribing and other corrupt practices and the BUYER will commit to prevent corruption, in any farm, by its officials by following transparent procedures.

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

1. **Commitments of the BUYER**

1.1 The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, 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 B1DDERs.

1.3 All the officials of the BUYER will report to the appropriate authority any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

1.4 In case any such preceding misconduct on the part of such official(s) is reported by the BIDDER to the BUYER with full and verifiable facts and the same is prima facie found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the BUYER and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings under the contract would not be stalled.

2. **Commitments of BIDDERs**

2.1 The BIDDER commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its Bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following:

2. 2 The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER, connected directly or indirectly with the bidding process, or to any person, 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 Commercial 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.

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

a. 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.

b. 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.

c. 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.

1. 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.
2. 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.
3. 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).

Shri Otem Dai, IAS (Retd.) Email: otemdai@hotmail.com	Shri Satyajit Mohanty, IPS (Retd.) Email: satyajitmohanty88@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.

(i) **Law and Place of Jurisdiction**

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

(ii) **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.

(iii) **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	For BIDDER
Name of the Officer.	Chief Executive Officer/
Designation	Authorised Signatory
Office / Department / Branch	Designation
State Bank of India.	

Witness	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-P

FORMAT FOR EMD BANK GUARANTEE

To:

EMD BANK GUARANTEE FOR
NAME OF SOFTWARE SOLUTION/ SERVICES TO STATE BANK OF INDIA TO MEET SUCH REQUIRMENT AND PROVIDE SUCH SOFTWARE SOLUTION/ SERVICES AS ARE SET OUT IN THE RFP NO. SBI/GITC/EIS2.0/2024-25/1221 DATED 14/10/2024

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 for Proposal to develop, implement and support _____(name of Software Solution/ Service) as are set out in the Request for Proposal SBI/GITC/EIS2.0/2024-25/1221 dated 14/10/2024.

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 not-withstanding 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 –

- 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)

- Our liability under these presents shall not exceed the sum of Rs._____/- (Rupees _____ Only)

- 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.

- 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.

- 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.

- 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.

- 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:

- Our liability under this Bank Guarantee shall not exceed Rs……/- (Rupees ……only)

- This Bank Guarantee shall be valid upto …….
- 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-Q

Data Processing Agreement

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

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

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

And

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

WHEREAS:

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

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

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

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

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation:

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

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

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

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

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

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

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

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

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

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

1.1.10 "EEA" means the European Economic Area.

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

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

1.1.13 "Data Transfer" means:

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

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

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

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

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

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

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

2. Processing of Personal Data:

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

2.2 Processor shall:

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

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

3. PROCESSOR OBLIGATIONS:

3.1 Processor Personnel:

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

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

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

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

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

3.2 Security:

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

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

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

3.3 Sub-Processing:

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

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

3.4 Data Subject Rights:

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

3.4.1Taking into account the nature of the Processing, Processor shall assist SBI by implementing appropriate technical and organisational measures (Processor obligations in Schedule 3), insofar as this is possible, for the fulfilment of SBI's obligations, as reasonably

understood by SBI, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

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

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

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

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

3.5 Personal Data Breach:

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

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

3.6 Data Protection Impact Assessment and Prior Consultation:

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

3.7 Deletion or return of Personal Data:

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

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

3.8 Audit Rights:

The Processor shall make available to State Bank of India and any supervisory authority or their representatives the information necessary to demonstrate its compliance with this Agreement and allow for and contribute to audits and inspections by allowing State Bank of

India, its Client, a supervisory authority or their representatives to conduct an audit or inspection of that part of the Processor's business which is relevant to the Services [on at least an annual basis (or more frequently when mandated by a relevant supervisory authority or to comply with the Data Protection Legislation) and] on reasonable notice, in relation to the Processing of Personal Data by the Processor.

3.9 Data Transfer:

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

3.10 Records:

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

3.11 Notify:

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

3.12 Agreement Termination:

Upon expiry or termination of this Agreement or the Services for any reason or State Bank of India's earlier request, the Procesor 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:

5.3.1This 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:	Business Continuity Management		
		Backup management		
		Desktop/system/server/network device hardening with baseline controls		
		Patch Management		
		Port Management Media Movement		
		Log Management		
		Personnel Security		
		Physical Security		
		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:	Firewall		
		WAF		
		IDS/IPS		
		AD		
		AV		
		NAC		
		DLP		
		Any other technology		
6	Whether rules are implemented on Firewalls of the Processor environment as per an approved process?			

S. No	Controls to be implemented		Compliance (Yes / No)	If under implementation, give date by which implementation will be done
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:	Web		
		Application		
		DB		
		Configuration		
		User access		
10	Whether the Processor maintains logs for privileged access to their critical systems?			
11	Whether privilege access to the Processor environment is permitted from internet?			
12	Whether the Processor has captive SOC or Managed Service SOC for monitoring their systems and operations?			
13	Whether the Processor environment is segregated into militarized zone (MZ) and demilitarized zone (DMZ) separated by Firewall, where any access from an external entity is permitted through DMZ only?			
14	Whether Processor has deployed secure environments for their applications for:	Production		
		Disaster recovery		
		Testing environments		
15	Whether the Processor follows the best practices of creation of separate network zones (VLAN Segments) for:	Web		
		App		
		DB		
		Critical applications		
		Non-Critical applications		
		UAT		

S. No	Controls to be implemented		Compliance (Yes / No)	If under implementation, give date by which implementation will be done
16	Whether the Processor configures access to officials based on a documented and approved Role Conflict Matrix?			
17	Whether Internet access is permitted on:	Internal servers		
		Database servers		
		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?			
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?			

S. No	Controls to be implemented		Compliance (Yes / No)	If under implementation, give date by which implementation will be done
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.			
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:	Right to Audit to SBI with scope defined		
		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.		
		Right to recall data by SBI.		
		Regulatory and Statutory compliance at vendor site. Special emphasis on section		

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

Appendix-R

Resource Requirement

TEAM STRUCTURE

The overall project requirement has been divided into 2 main parts i.e.

1. TILL IMPLEMENTATION OF PHASE 8 and

2. POST IMPLEMENTATION OF PHASE 8

For Implementation of APIs on the new Enterprise API Integration and Management Platform, there will be a dedicated team of architects, engineers, and testers, etc. who will be working on the delivery. The minimum number of L1, L2 and L3 has to be 25, 25 and 8 respectively.

The detailed indicative, non-exhaustive list of the roles is mentioned below:

Table R-1 Team Structure for

Role	KRAs	Role Experience	Qualifications
Program Manager	Act as the IT SPOC between SBI and SI/OEM team for the project. Manage engineering and testing best practices, standards, patterns and documentation Ensure quality and consistency of inventory artefacts for Infrastructure etc.	10+ years (Relevant Product/ Technology experience)	Full-time MBA/BE/B.Tech/ MCA or equivalent degree from a recognized University acceptable to the Bank. Preferred additional Tech certifications e.g. ITIL, CGEIT, etc. or equivalent certification acceptable to the Bank.
Lead Architect	Understand needs and As-Is to define system design and specifications Communicate system requirements to development and QA teams etc.	10+ years (Relevant Product/ Technology experience)	Full-time BE/B.Tech/ MCA or equivalent degree from a recognized University acceptable to the Bank. Preferred additional Tech certifications e.g. TOGAF, ITIL, PMP, etc or equivalent certification acceptable to the Bank.
Technical BA (For respective domains	Align new systems, programs, and applications with operations and services	5+ years (Relevant Product/	Full-time MBA/BE/B.Tech/ MCA or equivalent degree from a recognized University acceptable to the

like Retail, Corporate, Regulator / Govt / Fintech, Payments, Foreign Offices, JVs etc	Determine system efficiency by checking with internal departments and end users Monitor product and ensure compliance with IT industry regulation	Technology experience)	Bank. Required experience in Banking and financial services sector and technical knowledge.
API SME	Drive API gateway adoption, ensuring adherence to standards, and coordinating efforts across stakeholders	10+ years (Relevant Product/ Technology experience)	Full-time BE/B.Tech/ MCA or equivalent degree from a recognized University acceptable to the Bank. Preferred additional Tech certifications (e.g., Azure Dev, AWS, Oracle Appl. Dev, etc.) or equivalent certification acceptable to the Bank.
Integration Engineer	Program well-designed, testable, efficient code Execute full lifecycle feature development for Enterprise API Integration and Management Platform Document and maintain platform functionality	Senior: 5+ years; Junior: 3+ years (Relevant Product/ Technology experience)	Full-time BE/B.Tech/ MCA or equivalent degree from a recognized University acceptable to the Bank. Preferred additional Tech certifications (e.g., Azure Dev, AWS, Oracle Appl. Dev, etc.) or equivalent certification acceptable to the Bank.
QA Testers	Review requirements, specifications, and design documents to provide timely feedback Create structured testing plans and cases, document, and tack bugs Develop and execute automation scripts	Senior: 5+ years; Junior: 3+ years (Relevant Product/ technology experience)	Full-time BE/B.Tech/ MCA or equivalent degree from a recognized University acceptable to the Bank.
Project Leader	Manage the entire scope and timeline of the project to achieve targets. Communicate	10+ years (Relevant Product/	Full-time MBA/BE/B.Tech/ MCA or equivalent degree from a recognized University acceptable to the

	responsibilities and expectations to team members	Technology experience)	Bank. and Required experience in Banking and financial services sector and technical knowledge Preferred additional certification (e.g., PMP, ACP, CISM, CPM, etc.) or equivalent certification acceptable to the Bank.
Security Expert	Analyze IT specifications, assess security risks and implement controls/DR plans Install, configure and upgrade security software Secure networks through firewalls, inspect systems for vulnerabilities and monitor networks	Senior: 10+ years Junior: 5+ years (Relevant Product/ Technology experience)	Full-time BE/B.Tech/ MCA or equivalent degree from a recognized University acceptable to the Bank. Preferred additional Security certifications (e.g., CISSP, CISM, CISA, CEH, etc.) or equivalent certification acceptable to the Bank
Network Expert	Lead the implementation of network solution, upgrades, migration etc. Optimize network performance, Implement, and enforce network security policies, standards. Perform root-cause analysis for critical Incidents etc.	Senior: 10+ years Junior: 5+ years (Relevant Product/ Technology experience)	Full-time BE/B.Tech/ MCA or equivalent degree from a recognized University acceptable to the Bank. Preferred additional Network certifications (e.g., CISSP, CCNA, CCIE, CCNP, etc.) or equivalent certification acceptable to the Bank
Database Administrator	Lead the implementation of Database design and development, data migration, backup and recovery, performance monitoring and optimization of DB, carryout Database maintenance activity, security implementation, documentation and version control	10+ years (Relevant Product/ Technology experience)	Full-time BE/B.Tech/ MCA or equivalent degree from a recognized University acceptable to the Bank. Preferred additional Database certifications (e.g., OCP DBA, knowledge of OCI etc.) or equivalent certification acceptable to the Bank

For other generic roles:

Table R-2 Support Team

Role	Responsibility	Experience Required	Qualifications
L1 Support Engineer	Manage and troubleshoot platform and hosted APIs Ensure audit and statutory compliance and perform patch installations. Monitor platform performance and maintain documentation of recurring issues	3+ years (Relevant Product/ Technology experience)	Full-time BE/B.Tech/ MCA or equivalent degree from a recognized University acceptable to the Bank. (Lower academic level could be accepted for this role)
L2 Support Engineer	Address advanced technical problems, perform in-depth diagnostics, and manage API lifecycle tasks such as version control and policy management. Ensure security enforcement, rate limiting, and orchestration, and provide detailed analytics.	5+ years (Relevant Product/ Technology experience)	Full-time BE/B.Tech/ MCA or equivalent degree from a recognized University acceptable to the Bank. Preferred additional Tech certifications (e.g., Azure Dev, AWS, Oracle Appl. Dev, etc.) or equivalent certification acceptable to the Bank.

Appendix-S

MANUFACTURERS' AUTHORIZATION FORM

No. Date:

To:
(Name and address of Procuring Office)

Dear Sir:

Ref: RFP No. SBI/GITC/EIS2.0/2024-25/1221 dated 14/10/2024

We, who are established and reputable OEM / manufacturers / producers of _____ having factories / development facilities at _____ (*address of factory / facility)* do hereby authorise M/s _____ *(Name and address of Authorised Business Partner (ABP))* to submit a Bid, and sign the contract with you against the above RFP.

- We hereby extend our full warranty and support in accordance with the terms of the above RFP for the Products and services offered by the above ABP against the above RFP. Support (inclusive of Warranty/ AMC / resources) shall be on-site and comprehensive in nature having back to back support from us. In case Service Provider/ABP fails to provide Warranty/AMC/ATS/Services/resources or out of service due to any reasons, then we shall either provide ourselves or make alternative arrangement for the Warranty/ Service/AMC/ATS/resources of the Product(s) as required in accordance with the terms and conditions of the above RFP, at no extra cost and to the satisfaction of the Bank.
- We also undertake to provide any or all of the following materials, notifications, and information pertaining to the Products supplied by the ABP:
    - Such Products as the Bank may opt to purchase from the ABP, provided, that this option shall not relieve the ABP of any warranty obligations under the RFP; and
    - In the event of termination of production of such Products:
        1. advance notification to the Bank of the pending termination, in sufficient time to permit the Bank to procure needed requirements; and
        2. following such termination, furnishing at no cost to the Bank, operations manuals, standards and specifications of the Products, if requested.
- We duly authorise the said ABP to act on our behalf in fulfilling all installations, Technical support and maintenance obligations required by the contract.
- We hereby certify that we have read the clauses contained in O.M. No. 6/18/2019-PPD, dated 23.07.2020 order (Public Procurement No. 1), order (Public Procurement No. 2) dated 23.07.2020 and order (Public Procurement No. 3) dated 24.07.2020 regarding restrictions on procurement from a bidder of a country which shares a land border with India. We further

certify that we are not from such a country or if from a country, has been registered with competent authority. We certify that we fulfil all the requirements in this regard and our ABP is eligible to participate in the above RFP.

Yours faithfully,

(Name of OEM/Manufacturer / Producer)

Appendix-T

APPENDIX-T: TECHNICAL EVALUATION METRICS

Bidder response to Technical Evaluation

The bidder is expected to respond to the platform capabilities by mentioning the mode of availability of the specific capability (mentioned in the table below), along with supporting documentation mentioning clear feature details and explanation related to the option chosen, in terms of native or third party availability.

Table TE-1

Flag	Parameter Value	Description
A	Available out-of-the-box	Available as part of bidder's proposed solution from OEM (native or configured)
B	Available with customization	Available as part of bidder's proposed solution from OEM (but requires customization (managed by the bidder)
C	Functionality already implemented through 3rd Party tool/ software	Available as part of an integrated 3rd party solution (managed by bidder), costs included in the bid
D	Functionality compatible to be implemented through 3rd party tool/ software	Potential third-party providers indicated, bidder is responsible for integrating
E	Not available or not provided	Not available as part of proposed solution

T.1 Platform Capabilities (Weightage % – 42)

T.1.1 Feature Coverage

Table TE-2

Themes	Max Marks	Description	Marking Criteria

(1) API Design	**5**	• The platform should support async API design and documentation. • The platform should have clear segregation of System, Process and Experience layer. • The platform should provide support for design artefacts such as OAS (OpenAPI Specification), RAML (RESTful API Modelling Language) standards etc. • The platform should be capable of fetching design data from 3rd party API design tools in Swagger • The platform should be able to parse and validate the structure of API specification files against the schema of the specification language • The platform must have readymade patterns for common API design patterns, such as pagination, filtering, and sorting available • The platform must provide the capability of customization of components, such as API endpoints or data models • The platform should enable support for response callback APIs, to manage asynchronous API flows • The platform must provide an Integrated Development Environment (IDE) with tools and features for API development, testing, and debugging • The platform should enable integration with Gen AI tools for API design	**5 Marks:** The platform **provides more than or equal to 70% of the API Design-related features**. The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of customization or unavailability **2 Marks:** The platform **provides between 50% to 70% of the API Design- related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability. **0 Marks:** The platform **provides less than 50% of the mandatory API Design-related features.** The bidder lists out available features but no detailing is provided.

		• The platform should provide an OOTB (Out of the Box) web based and desktop-based platform for supporting design of APIs • The platform should enable automation of decision processes and services like document recognition.	
(2) API Implementation	**5**	• The platform should provide support for event streaming (Kafka, Solace, AWS Kinesis, Azure Eventhub etc.) and queuing platforms • The platform would support processing of business rules for transactions and corresponding routing • The platform components should have the capability to deliver bank specific customizations in quick time • The platform should provide drag and drop functionality, to allow developers to easily create and configure APIs by visually arranging components or modules • The platform should have low-code no-code features, Desktop based and web-based IDE. • The platform should have simplified developer portal & API catalogue. • The platform must provide an out of the Box developer portal with pre-built themes and templates, along with the ability to customize the portal	**5 Marks:** The platform **provides more than or equal to 70% of the API Implementation-related features.** The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of customization or unavailability. 2 Marks: The platform **provides between 50% to 70% of the API Implementation-related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability.

		with low code, along with self on-boarding with customized workflow with consumption metrics. • The platform should support plug & play for Java code.. • Error code and messages design mapping: Platform to provide and handle error code and messages design mapping customizations. • The platform should support multiple data transport protocols such as SOAP, HTTP, REST, File, JDBC (Java Database Connectivity) • The platform must be compatible with multiple data formats to cover JSON, CSV and XML files etc. • The platform should provide support for existing CI/CD pipeline for automated build, test, and deployment processes. • The platform should enable hosting of virtual APIs with 24/7 access to API playground. • The platform should enable simulation of issues and edge cases to support load testing, regression testing and performance testing • The platform should provide packaging support for API to convert into a deployable JAR or ZIP file • The platform should enable direct application of rate limiting and throttling policies directly to APIs • The platform should Circuit breaker functionality to handle and recover from failures in	0 Marks: The platform **provides less than 50% of the mandatory API Implementation-related features.** The bidder lists out available features but no detailing is provided.

		distributed systems, preventing cascading failures • The platform should enforce load balancing mechanisms to distribute incoming requests across multiple instances (instances activated through cloud service configuration) • The platform should support high throughput capabilities to handle a large volume of requests or transactions • The platform should ensure sanitization of user input to prevent security vulnerabilities such as SQL injection or cross-site scripting attacks • The platform should provide conducive implementation language support and less dependency on proprietary technologies like Java, .NET, etc. • The platform should have complete auto configuration of all components. • The platform should provide testing framework support for JUnit and others for automated testing of APIs. • The platform to provide an automatic API service discovery layer • The platform should support AI(GPT/LLM) based prompts to generate integration flows to improve developer productivity.	
(3) API Integration	**10**	• The platform should be able to route API messages to multiple downstream applications extensively.	10 Marks: The platform **provides more than or equal to 70% of the API Integration-related features.**

		• The platform should be able to transform the messages between multiple data formats • The platform should have ESB and messaging components to support interoperability among different applications. different channels, downstream service providers, external integrations, and existing EIS. • The platform should support all relevant data formats e.g. JSON, XML, Strings, Text, CSV, Flat File format, Fixed Width format, COBOL, JSON, YAML, Custom Type, Excel etc. • The platform should support multiple data type support including BLOB. • The platform should support multiple transport protocols such as SOAP & Webservices, JMS, HTTP, RESTful, File, Websocket, JDBC, TCP/UDP Socket, OData, SFTP & FTPS, ISO Base24 Fix length etc. • The platform should support UDDI specification to publish and discover information about web services. • The platform should have the capability to convert one protocol to another protocol. • The platform to have out-of-the-box connector to connect to downstream applications like CBS, RLMS, etc. • The platform should have the ability to integrate with existing governance platform of the Bank. e.g. PIMS, SIEM, DAM, etc.	The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of customization or unavailability. 4 Marks: The platform **provides between 50% to 70% of the API Integration-related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability. 0 Marks: The platform **provides less than 50% of the mandatory API Integration-related features.** The bidder lists out available features but no detailing is provided.

		• The platform should provide the flexibility to build custom connectors with SDK.SDK for custom API policies. • The platform should have readymade palette for integration with JDBC , FTP, SFTP, TCP etc. • The platform should provide support for unit testing and code coverage. • Exposed APIs should be compatible for any internal systems for ease of integration (built as RESTful) • Integration support with external monitoring platforms to provide health status of services. • API Validation/simulation • The platform should have the capability of decision automation e.g., Decision based on thresholds/defined parameters. • B2B Integration. EDI Standards Support (X12, EDIFACT, XML, JSON, File etc.) . Support for EDI specific transports (HTTP/s, FTP/SFTP, AS2). Partner Onboarding and Management. B2B transaction security, insights and management. • APIs cataloguing and auto discovery capability to enable reuse of existing APIs • The platform should enable AI based data transformation tooling, allowing for automatic conversion and manipulation of data formats, structures, or content.	

		• Virtualization [to test your API early and often] • The platform should support Intelligent Document Processing like compression, extraction. • Seamless integration with serverless computing platforms covering both cloud and on-premise setup	
(4) API Governance	**5**	• Unified API life cycle management: The platform should be able to manage the end-to-end API lifecycle. • Service level agreements • API design compliance (OWASP and Open banking standards) • The platform uses swagger to design, build, and document the APIs • API implementation and policy adaption compliance. • The platform provides API versioning capability via API Manager, enabling easy management of different API versions • The platform supports JWT (JSON Web Token) and OpenID Connect token validation • The platform should provide OOB (Out of the Box) Quality of Service (QoS) policies such as service availability, performance, integration	**5 Marks:** The platform **provides more than or equal to 70% of the API Governance-related features**. The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of customization or unavailability. 2 Marks: The platform **provides between 50% to 70% of the API Governance-related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability.

		• Custom governance rule sets	**0 Marks:** The platform **provides less than 50% of the mandatory API Governance-related features.** The bidder lists out available features but no detailing is provided.
(5) API Observability	**5**	• The platform should support logging based on severity & criticality of the events like Debug, Warning, Info, Fatal, Exception etc. • The platform should have the capability to masking the Audit log as per security requirements. • The platform should have the ability to extract data for forensics. • Meta-Data Support • End to end monitoring: The platform should have End to end monitoring capability including observability (resource availability, stability, and performance), predictive analytics and proactive response along with operational workflow. • The platform should provide OOB (Out of the Box) dashboards for monitoring of the API health	**5 Marks:** The platform **provides more than or equal to 70% of the API Observability-related features.** The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of customization or unavailability.
			2 Marks: The platform **provides between 50% to 70% of the API Observability-related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability.

		• The platform should be able to generate reports based on the collected data in the form of dashboards, PDF, XLS to be used for support, resilience, Monitoring. • The platform should provide traceability capabilities to track the impact and history of corrective actions taken on the system • The platform should cater to customized monitoring requirements like connecting to ROC for improved observability. • The platform should support automated notifications during request compatibility issues, API token failures, high response time with direct connection to ITSM for ticket raising • The platform should provide real-time data analysis and visualization for live tracking of performance • The platform database should collect machine data, part production data, and quality data to enable effective business performance management • The platform should provide log management capabilities to collect, store, and analyze log data generated by various components and systems • The platform should support log creation for detailed information on behavior of applications and integrations • Custom analytics reports and AI-based anomaly detection	**0 Marks:** The platform **provides less than 50% of the mandatory API Observability-related features.** The bidder lists out available features but no detailing is provided.

		should be supported by the platform • The platform should automatically track and assign corrective actions to appropriate personnel or teams • The platform should provide analytics capabilities to monitor and analyze the usage, performance, and effectiveness of APIs • The platform should support single pane monitoring of all internal and external APIs • The platform should provide visualization capabilities to depict the network topology and connections between various components and systems	
(6) API Monitoring	**5**	• The platform should provide single pane of glass for applications, microservices, Monitoring and Analytics. • Async API Monitoring. • The platform should provide centralized monitoring for Integration and API Management components • The platform should provide Alerts, Log Management, Reports, Health Check Monitoring, Business activity monitoring via Custom Metrics, Application network	**5 Marks:** The platform **provides more than or equal to 70% of the API Monitoring-related features.** The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of customization or unavailability.

		visualization, API and integration analytics. • The platform should have capability to trace end to end customer interactions. • Customized monitoring requirements like connecting to ROC for improved observability. • The platform should have out of box dashboard for unified APIs, orchestrated APIs, Common APIs, etc. • Auto-Escalation. • Auto-Ticketing. • The platform should provide Real-time data analytics. • The platform should provide Business performance measurement for banking services • Reuse & ROI Metrics.	**2 Marks:** The platform **provides between 50% to 70% of the API Monitoring-related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability.
			0 Marks: The platform **provides less than 50% of the mandatory API Monitoring-related features.** The bidder lists out available features but no detailing is provided.
(7) API Commercialization	**5**	• The platform should be able to support charging models. • The platform should provide support for multiple models of API commercialization	**5 Marks:** The platform **provides more than or equal to 70% of the API Commercialization-related features.** The bidder provides comprehensive documentation listing out available features with

			detailed rationale of availability, extent of customization or unavailability.
			2 Marks: The platform **provides between 50% to 70% of the API Commercialization-related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability.
			0 Marks: The platform **provides less than 50% of the mandatory API Commercialization-related features.** The bidder lists out available features but no detailing is provided.
(8) API Publishing	**5**	• The platform should be able to download APIs as connectors for reuse. • The platform should be able to discover and reuse existing assets (event driven APIs). • Availability of reusable asset of API management for data mapping, transformation, orchestration and business logic flows • Central asset repository to keep track of APIs and assets built	**5 Marks:** The platform **provides more than or equal to 70% of the API Publishing-related features.** The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of customization or unavailability.

		on platform to manage API, examples, connectors • The platform should enable Auto documentation of APIs with standardized documentation • The platform should support auto generation of developer portal from API schemas and meta-data	**2 Marks:** The platform **provides between 50% to 70% of the API Publishing-related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability.
			0 Marks: The platform **provides less than 50% of the mandatory API Publishing-related features.** The bidder lists out available features but no detailing is provided.
Total	**45**		

T.1.2 Technical Capabilities

Table TE-3

Themes	**Max Marks**	**(Category #) (Mandatory (M)/Essential (E)/Optional (O)) Requirements**	**Marking Criteria (5/5), (10/10), (15/15), (20/20), (30/30), (40/40)**
(9) Messaging	**5**	• The platform should provide Message broker and queueing pattern. Advanced messaging capabilities, including routing, queuing for message storage and retrieval • The platform should support unicast and broadcast.	**5 Marks:** The platform **provides more than or equal to 70% of the API Messaging-related features.** The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of

		• The platform should provide integration with external messaging platform: Kafka, MQTT, JMS, MQ and others, allowing for seamless integration and communication • The platform should provide support for converting data from one format or protocol to another, such as SOAP to REST, XML to JSON, JSON to XML, and XSL etc..	customization or unavailability. **2 Marks:** The platform **provides between 50% to 70% of the API Messaging-related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability. **0 Marks:** The platform **provides less than 50% of the mandatory API Messaging-related features.** The bidder lists out available features but no detailing is provided.
(10) Deployment	**5**	• All components like API Gateway, ESB etc. should be fully compatible and scalable in the Bank's current Private cloud (ex: Meghdoot) infrastructure. • The platform should provide support for geo-redundant deployment strategy. • The platform should provide support for integrating with CI/CD	**5 Marks:** The platform **provides more than or equal to 70% of the API Deployment-related features.** The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of

		pipeline platforms like: Jenkins, Maven, Azure etc. and other available CICD tools in the Bank. • The platform should provide support for Maven, Ant, etc. • The platform should be cloud native & cloud ready and have the capability to be deployed on demand. • Managed cloud deployment. • Public/ private cloud deployment with no vendor lock-in. • The platform should be CNCF Compliant: Cloud Native Computing Foundation (CNCF) compliant Kubernetes deployment - Same code to work in all environments. • The platform should provide support for blue/green deployment, allowing users to create and manage two identical environments (blue and green) • The platform should provide configurable automatic back up & restoration mechanism. • The platform to have inbuilt DevSecOps capability. • The platform should support on premise deployment and able to provide all features on premise and have no linkages to	customization or unavailability. **2 Marks:** The platform **provides between 50% to 70% of the API Deployment-related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability. **0 Marks:** The platform **provides less than 50% of the mandatory API Deployment-related features.** The bidder lists out available features but no detailing is provided.

		models/algorithms in cloud. • The platform should provide capabilities to override API response calls in case of system downtimes or issues, and process data later as batches • The platform should provide support for infrastructure as code (IAC)	
(11) Scalability	**5**	• The platform should be capable of handling the volume of the Bank and to be the single API gateway for the Bank. • The platform should support Auto scale and self-heal and auto repair capabilities. • The platform should provide Non-blocking I/O, Microservices with containerization Support, Streaming capabilities, Parallel processing. • The platform should have the capability to configure tuning parameters for clustering and high availability. • The platform should be able to handle TPS of more than 7000. • The platform should have support for asynchronous mechanism enabled for improved scalability and resilience. • The platform should be capable of rate limiting and	**5 Marks:** The platform **provides more than or equal to 70% of the API Scalability-related features.** The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of customization or unavailability. **2 Marks:** The platform **provides between 50% to 70% of the API Scalability-related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability.

		throttling between different consumers • The platform should provide horizontal scaling capability to accommodate increased traffic and workload • The platform should provide streaming capabilities to allow for efficient transfer of large amounts of data in real-time	**0 Marks:** The platform **provides less than 50% of the mandatory API Scalability-related features.** The bidder lists out available features but no detailing is provided.
(12) Latency	**5**	• The platform should be able to provide quick average turnaround time of API delivery • The platform API gateway should be able to support more than 4 MB payload size • The platform should have the capability of Payload compression. • The platform to have support for Service Mesh capability for high availability. • The platform to have Out of the box resiliency for network failures and service communication by facilitating throttling and circuit breaker architectural patterns. • The platform should support Maximum Payload size	**5 Marks:** The platform **provides more than or equal to 70% of the API Latency-related features.** The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of customization or unavailability.
			2 Marks: The platform **provides between 50% to 70% of the API Latency-related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability.

		• The platform should have capabilities of Cache management. • The platform to have the batch run capability. • Distribution of traffic across mesh. Easily configurable API timeouts based on API scenarios.	**0 Marks:** The platform **provides less than 50% of the mandatory API Latency-related features.** The bidder lists out available features but no detailing is provided.
(13) Architecture	**5**	• The platform should have capability for orchestration by configuration i.e. multiple APIs from different applications with minimum efforts and timelines. • Drag/ drop based orchestration • Easy request response transformation • The platform should have capability for API choreography - process where multiple subscribers react to a single event, using the data received for their own purposes • The platform should support API led microservices and journey aggregations. • The platform should have the capability of event based triggering support mechanism and support event driven architecture. • The platform to support Service Component Architecture (SCA) - a set of specifications at describe a programming model for	**5 Marks:** The platform **provides more than or equal to 70% of the API Architecture-related features.** The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of customization or unavailability.
			2 Marks: The platform **provides between 50% to 70% of the API Architecture-related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability.

		building applications and systems using a Service-Oriented Architecture (SOA) • Availability of ESB within platform should support legacy applications and enable seamless integration with modern architectures • ESB should serve as a single-entry point for external systems through an API gateway. • ESB should support orchestration and integration of loosely coupled components, especially for legacy applications • The platform should provide complex event recognition capability, allowing the system to identify and respond to complex events. • The platform should support streaming of events, enabling real-time processing and analysis of event data. • The platform should provide asynchronous API communication support, allowing for non-blocking and event-driven interactions between components or services • The platform should provide the capability to compress payloads to save bandwidth and reduce latency in some situations • Service mesh architecture to provide a dedicated infrastructure layer for managing service-to-service communication, ensuring scalability, reliability, and observability	**0 Marks:** The platform **provides less than 50% of the mandatory API Architecture-related features.** The bidder lists out available features but no detailing is provided.

		• The platform should support API request queuing, retrieval and routing options to be available to manage peak transaction workload • The platform should support for multi-clustered gateways and micro gateways for customized entry points per use case • The platform should support micro gateway for accessing individual microservice through a separate gateway • The platform should have a clearly defined payload capacity at LB and WAF levels for correct response capturing and smooth transaction flow • The platform should enable Master API to be bifurcated into multiple smaller APIs endpoints for smooth functional changes and faster change deployments	
(14) Security	**5**	• The platform should provide message level encryption support to protect the confidentiality and integrity of data during transmission • The platform should enable async API Management and Security. • The platform should have a component on Security Module along with enterprise level platform,	**5 Marks:** The platform **provides more than or equal to 70% of the API Security-related features.** The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of customization or unavailability.

		application and API security adoption. • The platform should provide support for multiple security protocols. • The platform should provide support for multiple encryption algorithms protocols like AES 256, SHA, 256 etc. • The platform should support OOTB policies for message threat protection, IP allow/blocklist and header injection/removal. • JWT and OIDC token validation. • OOTB Quality of service policies. • The platform should be able to support hardware security module (HSM) • The platform's Compliance should be equivalent to payment systems including PCI DSS by not storing card data on the platform • The platform should support Tokenization, Nonrepudiation mechanisms e.g. JWT, OAuth2 • The platform should provide the ability to handle electronic signature verification e.g., Digi-sign verification. • The platform should support field level encryption, basic authorization, fine grained authorization and identity management. • The platform should support all access management related requirements of the Bank.	**2 Marks:** The platform **provides between 50% to 70% of the API Security-related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability. **0 Marks:** The platform **provides less than 50% of the mandatory API Security-related features.** The bidder lists out available features but no detailing is provided.

		• The platform should support native feature richness for authorization and authentication: OAuth2, OpenID Connect, other protocols • The platform should provide secure configuration files. • The platform should provide third party OIDC integration capability. • The platform should support logging with meta data and provide log extraction for analysis • Encryption or masking of API objects or data points until consumed through code workflow within systems • The platform should support WAF, TLS v1.2,v1.3 etc. • WAF supervision for API endpoints to be domain based for preventing unauthorized or dummy transactions • The platform should support multiple encryption algorithms protocols such as RSA, AES, hashing etc.. • The platform should support SAML (Security Assertion Markup Language) for secure single sign-on (SSO) and identity federation • The platform should provide Message level encryption, Field level encryption, Basic Auth, SAML, Fine grained authorization, Identity management • The platform should provide identity	

		management features to manage user identities, including user provisioning, authentication, and authorization • API vulnerability detection capabilities like injection, broken authentication, and insecure deserialization. • Vulnerability detection for incidents such as SQL injection, cross-site scripting (XSS), and XML external entity (XXE) attacks • OOB (Out of the Box) support for mutual TLS (Transport layer security), for encryption and authentication of all communication between services. • The platform should enable API vulnerability detection capabilities like **injection, broken authentication, and insecure deserialization.** • The platform should provide vulnerability detection for incidents such as **SQL injection, cross-site scripting (XSS), and XML external entity (XXE) attacks** • The platform should provide a real-time central configuration file of API endpoints to manage API activeness and smooth service degradation. • API module and other systems should have relevant IP and port whitelisted for managing the API consumption and security	

		• The platform should provide VPN tunnel for providing a secure messaging channel for communication	
(15) Third-Party Integrations	**15**	• Managing APIs deployed anywhere. • Third party identity provider integration capability with audit trails. • The platform should support integration with third-party OpenID Connect (OIDC) providers for user authentication • The platform supports integration with third party monitoring tools like Heal, Dynatrace and other similar tools • The platform should have out of the box connectors with easy integration with third-party services such as Amazon S3, Jira etc. to facilitate smooth interaction of APIs with external tools • The platform should support API Auto-cataloguing. • The platform should provide API Auto discovery.	**15 Marks:** The platform **provides more than or equal to 70% of the API Third party integration-related features with minimum number of OEMs.** The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of customization or unavailability.
			7 Marks: The platform **provides between 50% to 70% of the API Third party integration-related features with minimum number of OEMs.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability.
			0 Marks: The platform **provides less than 50% of the**

			mandatory API Third party integration-related features with minimum number of OEMs. The bidder lists out available features but no detailing is provided.
(16) Compliance with Standards and Regulations	**5**	• The platform should follow **Global Standards like Open Banking, BIAN standards, etc.** • The platform should follow **Global Specifications like OpenAPI**	**5 Marks:** The platform **provides more than or equal to 70% of the Compliance with Standards and Regulations-related features.** The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of customization or unavailability.
			2 Marks: The platform **provides between 50% to 70% of the Compliance with Standards and Regulations-related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability.
			0 Marks: The platform **provides less than 50% of the mandatory Compliance with Standards and**

			Regulations-related features. The bidder lists out available features but no detailing is provided.
(17) Portability	5	• The platform should be able to support various **version control tools e.g. Jenkins** • The platform to have ability to deploy on **containerized based architecture.** • **Vendor and cloud portability** to reduce partner lock-ins for products • Presence and maturity of platform APIs to enable **Infrastructure-as-Code (IaC)**	**5 Marks:** The platform **provides more than or equal to 70% of the Portability-related features.** The bidder provides comprehensive documentation listing out available features with detailed rationale of availability, extent of customization or unavailability.
			2 Marks: The platform **provides between 50% to 70% of the Portability-related features.** The bidder provides comprehensive documentation listing out available features with limited details rationale of availability, extent of customization or unavailability.
			0 Marks: The platform **provides less than 50% of the mandatory Portability-related features.** The bidder lists out available features but no detailing is provided.
Total	**55**		

T.2 Bill of Materials (Weightage % – 8)

Table TE-4

Criteria	Indicative Criteria	Max Marks	Scoring Guidelines	Marking criteria
Infrastructure Sizing Reference Table: T.2.1	The major components are listed, and their description provided	20	Proposed solution not well detailed and not properly contextualized to suit the bank's requirement. Technology components are described in an ad-hoc manner	5
	High level of details on the components, description, and other requirements		The proposed solution is contextualized to fulfill the requirements - Technology components are described in detail and structured according to the Bank's requirements	10
	Maximum level of details on the makes, description, and other requirements		The proposed solution is contextualized to fulfill the requirements - Components are described in detail and structured according to the Bank's requirements - Detailed design examples with a view to fulfill the requirements are provided	20
Applications/ software/products	The major components are listed, and their description provided	50	Proposed solution not well detailed and not properly contextualized to suit the bank's requirement. Technology components are described in an ad-hoc manner	10
	High level of details on the components, description, and other requirements		The proposed solution is contextualized to fulfill the requirements - Technology components are described in detail and structured according to the Bank's requirements	20
	Maximum level of details on the makes, description, and other requirements		The proposed solution is contextualized to fulfill the requirements - Components are described in detail and structured according to the Bank's requirements	50

	All components of Integrated Product Suit are from less number of OEMs.		- Detailed design examples with a view to fulfill the requirements are provided - All components of Integrated Product Suit are from less number of OEMs.	
Team construct (Team size, experience, technical qualification)	The major roles are listed, and their numbers provided	30	Proposed team construct not well detailed and not properly planned to suite the requirement. -team roles and numbers are described in an ad-hoc manner	05
	High level of details on the team construct with details on phase wise composition.		Proposed team construct is well detailed and properly planned to suite the requirement. -Team roles and numbers are described for the starting phase.	15
	Maximum level of details on the roles, team construct with details on phase wise composition and other requirements		The proposed team construct is highly detailed and contextualized to phase-wise plan to fulfill the requirements. - The roles and responsibilities are described in detail and structured according to the technology proposed and Bank's requirements	30
	Total Marks	100		

T.2.1

Infrastructure Sizing

As per your requirement given in RFP, the following Infrastructure will be required for implementing the Enterprise API Integration and Management Platform:

Table TE-5

Year	Region	Estimated Infrastructure Requirement		
		Compute (vCore)	RAM (in GB)	Storage (in GB)
1-5	DEV			
1-5	SIT			
1-5	UAT			
1-5	Pre-PROD			
1	PROD			
1	DR			
2	PROD			
2	Near-Prod			
2	DR			
2	Near-DR			
3	PROD			

3	Near-Prod			
3	DR			
3	Near-DR			
4	PROD			
4	Near-Prod			
4	DR			
4	Near-DR			
5	PROD			
5	Near-Prod			
5	DR			
5	Near-DR			

T.3 Implementation approach (Weightage % – 11)

T.3.1 Planning

Table TE-6

Criteria	Indicative Criteria	Max Marks	Scoring Guidelines	Marking criteria
Approach	Description of the methodology to maximize the delivery in the short term, implement zero technical debt and accomplish the objective faster than expected	10	Basic explanation with no concrete examples.	2
			Non obvious examples detailed. Complete definition including metrics and past experiences	5
			Complete description including use cases, KPIs, metrics, past experiences, and an entire detailed planning for the whole project	10
Implementation Plan	detailed Project plan highlighting timelines required for the delivery, Installation of software, Cloud etc., Development, Testing, UAT, Implementation, support etc.	10	Basic project plan with no concrete highlights of milestones.	2
			Non obvious examples detailed. Complete detailed project plan with definition including milestones.	5
			Complete description including use cases, KPIs, metrics, past experiences, and an entire detailed planning for the whole project	10

Agility	Plan to ensure to incremental and effective development aligned in set of ceremonies	10	Less than the expected number of ceremonies defined - The response is not covering the basic agile product development principles, including DevSecOps,automated testing and deployment, integrated security, and release management. - Plan to train and upskill the team on agile practices is not provided - Requirement life cycle management, task allocation and task tracking proposed to be managed	2
			expected number of ceremonies defined the response is covering the basic agile product development principles laid down in the RFP - proposal to train their team on agile development practices and principles at the beginning of the project. Regular trainings to upskill resources on new practices - Requirement life cycle management, task allocation and task tracking Proposed to be captured in a centralized repository/drive by the bidder	5
			More than the expected number of ceremonies defined - The response is introducing additional agile development practices, principles, agile team structures and communication methodology for overall project agility - team already is agile certified before beginning of the project. Regular trainings planned for the team and bank employees for upskilling resources on new practices	10

			- Requirement life cycle management, task allocation and task tracking proposed to be captured in an agile project planning tool like JIRA/ confluence	
Total Marks		30		

T.3.2 Delivery

Table TE-7

Criteria	Indicative Criteria	Max Marks	Scoring Guidelines	Marking criteria
Quality Assurance	Ability to ensure product quality and adherence to execution timelines	15	Less than the expected number of testing mechanisms defined - Manual quality checks proposed like code review, report generation, defect logging, execution of cross platform test cases - Less than 60% code coverage - No productivity improvements/ testing efforts savings proposed - No designated resources for ensuring quality control	3
			Testing mechanisms covered in proposal - Automated quality checks proposed like code review, report generation, execution of cross platform test cases (<80% test cases automated). Defect logging done manually in defect management tool - 60%-80% code coverage - 5%-10% productivity improvements/ testing efforts savings proposed - Designated resources with necessary skills included as part of the team for ensuring quality control	7

			Proposal includes more than the expected number of testing mechanisms defined - Automated quality checks proposed like code review, code vulnerability check, report generation, execution of cross platform test cases (>80% test cases automated), Defect logging in defect management tool. Roadmap for automation and KPIs for roadmap implementation included by the Bidder - >80% code coverage - 10+% productivity improvements/ testing efforts savings proposed with roadmap and KPIs defined - Designated resources with necessary skills backed by the quality control COE and tools included as part of the solution for ensuring quality control	15
Training	Delivery and frequency of trainings conducted. Training quality, learning experience and fitment of trainings	5	Plan to deliver the Trainings is not provided - Generic trainings planned for the team	1
			Training Plan provided with type of trainings and content of trainings to be delivered. trainings planned at the beginning and end of project. - Customized Training content planned for Bank employees and development resources. Training is in line with Tech requirements offering certification courses aimed at building digital skills	2
			Training plan provided with type of trainings and content of trainings to be delivered. Frequent trainings planned in line with project milestones that meet the training needs of all user groups. Training plan leverages existing learning resources and learning portal. - SBI specific training content planned for Bank employees and team development resources. Training process is gamified and in line with Tech requirements offering certification courses aimed at digital skill building. Trainings to enable smooth Knowledge Transfer for new members.	5
Documentation	Technical documentation of the project deliverables and Documen	10	Agrees to documentation but List and format of documents not defined	2
			Proposed list of technical documents is shared. Plan to review the technical documents in place - Plan to create documents that capture the business requirements, project deliverables and development milestones	5

	ts related to project management processes		Proposed list of technical documents to be created following the bank defined templates is shared. There is a plan to review and manage the documentation throughout the project lifecycle and ensure reusability, document sharing and version management - Plan to create documents following a structure and template defined by the bank to capture requirements, project deliverables and development milestones. Plan to update the documents as the project evolves, maintain document versioning, and have a well-defined approval and sharing mechanism in place	10
Compliance	Security frameworks being followed and understanding of the bank security controls and regulatory norms	10	- Security frameworks to be followed are not clear - Unclear understanding of the Regulatory standards and Security controls applicable to the Bank	2
			Security frameworks to be followed are well defined. Plan to ensure compliance through automated checks, reviews gates, checklists in place - Demonstrate understanding of the regulatory standards and security controls applicable to the bank	5
			Security frameworks to be followed are well defined. Plan to ensure compliance through automated checks, reviews gates, checklists in place. Proposed a plan to strengthen the security posture by following industry leading security standards and improve the bank's resilience - Demonstrate strong understanding of the regulatory standards and security controls applicable to the bank. Plan to evolve the security stance with industry leading best practices as required during the Project delivery	10
Total Marks		40		

T.3.3 Support

Table TE-8

Criteria	Indicative Criteria	Max Marks	Scoring Guidelines	Marking criteria
Enterprise Support	Practice of supporting IT systems/applications which are being used to resolve issues quickly with at least 3 levels of support along with	10	Provide support coverage of 8X7X365 equivalent or less with less than 3 levels of support	2

	community and online resources. Integration support capabilities with India-based support at all the levels available		Provide support coverage of 18X7X365 equivalent or less with less than 3 levels of support	5
			Provide support coverage of 24X7X365 equivalent or less with 3 levels of support	10
Online Resources and Community		5	Limited Online resource and community available	1
			considerable Online resource and community available	2
			comprehensive Online resource and community available	5
System Integrator Support Capabilities		5	limited System Integrator Support Capabilities	1
			Optimum System Integrator Support Capabilities	2
			Strong System Integrator Support Capabilities	5
India-based Product Support		10	<50% of India Based support available	2
			<75% of India Based support available	5
			>=80% of India Based support available	10
	Total Marks	30		

T.4 Bidder Evaluation (Weightage % – 19)

Table TE-9

Criteria	Indicative Criteria	Max Marks	Scoring Guidelines	Marking criteria
Partnerships	Access to partnerships/ vendors	45	Bidder has leverage and can utilize technology and services of each of the OEM components recommended in this project for min 3 years	10
			Bidder has leverage and can utilize technology and services of each of the OEM components recommended in this project for min 5 years	20
			Bidder has leverage and can utilize technology and services of each of the OEM components recommended in this project for min 10 years	45
Portfolio and References	Contacts of previous companies in which the Bidder has completed projects for BFSI in India and across the globe	30	Min 2 Indian and 2 Global relevant large-scale implementations	10
			2-5 Indian and 2-5 Global relevant large-scale implementation and contacts details from past distinct BFSI clients has been provided in the format mentioned in Appendix-N	15
			More than 5 Indian and 6 or more Global relevant large-scale implementation and contacts details from past distinct BFSI clients has been provided in the format mentioned in Appendix-N	30
Eco-System Knowledge	Knowledge of the BFSI in general and specifically the knowledge of SBI eco-system	25	High-level eco-system knowledge	05
			Optimum eco-system knowledge with knowledge of the network, systems and applications available in the bank and their functional capabilities	10
			In-depth knowledge of the network, systems and applications available in the bank and their functional capabilities	25
Total Marks		100		

T.5 Tools Demo (Weightage % –12)

Table TE-10

Dimension	**Criteria**	**Max Marks**	**Reference**
Understanding of the scope of work	Coverage and depth of the dimensions	10	Appropriate reference to documents submitted as part of previous sections
Proposed approach and roadmap, including architecture, handling scale, and critical applications		20	
Team structure across phases, key profiles, time commitment		20	
Relevant customer credentials including case studies, demos		20	
Partnerships with key OEMs (hardware, software, solutions), integration with external agencies		10	
Existing know-how, reusable components, boilerplate code that can be deployed for the bank (demos preferable), sharing of IP		10	
Foreseen risks and mitigation approach		10	
Total Marks		100	

T.6 Reference Call and/ or Visit (Weightage % – 8)

Table TE-11

Dimension	**Criteria**	**Max Marks**
Size, scope, and relevance of the reference	Coverage and depth of the dimensions	20
Tech architecture including scalability, availability, performance, etc.		30
Implementation approach including MVP, timelines, agile methodology		30
Adherence to regulatory, compliance, security, risk and other mandatory requirements		20
	Total Marks	100

Appendix-U

PERFORMANCE CERTIFICATE

(To be provided on letter head / official mail ID of the issuing company)

The Deputy General Manager
EIS 2.0 Department
State Bank Global IT Centre

Date: __/__/____

Sir,

Reg: RFP for Software Solution & Services for Enterprise API Integration and Management Platform

This is to certify that following components, in form of Integrated Product Suite / Platform, has been implemented and is in use at our organization since _____ (date).

Sr no	Integrated Product Suite Components	Name of Product / Module / Layer	OEM Name
1	API Gateway		
2	API Management		
3	Enterprise Service Bus (ESB)		
4	Message Queuing Service		
5	API Orchestration		
6	API Security		
7	Integrated Product Monitoring		

Around _____ number of orchestrated & individual APIs integrated with ____ applications (internal / external) has been successfully integrated / developed / migrated in the Platform.

The performance of the Platform as well as OEM support are satisfactory.

The certificate is issued on the specific request of the company.

Signature of Authorised Signatory
Name of Signatory:
Designation:
Email Id:
Mobile No:
Telephone No:
Seal of Company

Glossary

Abbreviation	Full Form
API	Application Programming Interface
BFSI	Banking, Financial Service and Insurance
CI/ CD	Continuous Integration and Continuous Deployment
DAM	Database Activity Monitoring
DevSecOps	Development, Security, and Operations
EIS	Enterprise Integration Service
ESB	Enterprise Service Bus
IAM	Identity and Access Management
ITSM	Information Technology Service Management
KEDB	Known Error Database
N-DR	Near Disaster Recovery
N-PR	Near Production
OEM	Original Equipment Manufacturer
OOTB	Out Of The Box
Pre-Prod	Pre-Production
PROD	Production
PIMS	Personal Information Management System
ROC	Resilience Operations Centre
SDK	Software Development Kit
SIEM	security information and event management
SIT	System Integration Testing
SOC	Security Operations Center
UAT	User Acceptance Testing