REQUEST FOR PROPOSAL
FOR PROCUREMENT OF END-TO-END SOLUTION FOR ANALYTICAL LAYER PLATFORM UNDER FRAUD RISK MANAGEMENT (FRM) FRAMEWORK

Ref: SBI:RMD/PRMD/2025-26/01
Dated : 02/01/2026

State Bank of India
Proactive Risk Management Department
Sanganer, Tonk Road,
Jaipur – 302015

1. Schedule of Events

Sl No	Particulars	Remarks
1	Contact details of issuing department (Name, Designation, Mobile No., Email and office address for sending any kind of correspondence regarding this RFP)	Shri Paramjeet Singh Sodhi GM (PRMD) Proactive Risk Management Department Sanganer, Tonk Road, Jaipur – 3002004 Email: gm.prm@sbi.co.in dgm.prmbi@sbi.co.in agmit.prm@sbi.co.in
2	Bid Document Availability including changes/amendments, if any to be issued	RFP may be downloaded from Bank's website https://www.sbi.co.in procurement news from 02.01.2026 (05:00 PM) to 23.01.2026 (03:00 PM)
3	Last date for requesting clarification	Upto 03:00 PM (time) on 12.01.2026 (date) All communications regarding points / queries requiring clarifications shall be given in writing or by e-mail.
4	Pre - bid Meeting at (venue)	From 03:00 PM to 04:00 PM (time) on 13.01.2026 (date) at (Venue to Be advised if conducted in-person) or through online meeting
5	Clarifications to queries raised at pre-bid meeting will be provided by the Bank.	On 19.01.2026 (date)
6	Last date and time for Bid submission	Upto 03:00 PM (time) on 30.01.2026 (date)
7	Address for submission of Bids	https://etender.sbi/SBI
8	Date and Time of opening of Technical Bids	05:00 PM (time) on 30.01.2026 (date) 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 Price Bids	Price bid of technically qualified bidders only will be opened on a subsequent date.
10	Tender Fee	Rs.25,000/- (Rupees Twenty Five Thousand Only) The Tender Fee will be deposited in form of the Demand Draft. Tender fee will be non-refundable.
11	Earnest Money Deposit	Rs. 2,00,00,000 (Rupees Two Crores Only) 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.**
12	Bank Guarantee	@5% of the cost quoted in the Total cost of Operations (TCO) Performance Security in form of BG should be valid for 5 year(s) and three months from the effective date of the Contract.
13	Contact details of e-Procurement agency appointed for e-procurement	1. Sh. Akhlad Rajput Email: akhlad.rajput@eptl.in Phone: +91- 7859800624 2. Sh. Nandan Valera Email: Nandan.v@eptl.in Phone: +91- 9081000427 3. Nithya Vallavar Email: Nithya@eptl.in Phone: +91- 7859800609

Table of Contents

Part-I

Part-II

2. INVITATION TO BID

i. **State Bank of India** (herein after referred to as **'SBI/the Bank')**, having its Corporate Centre at Mumbai, various other offices (LHOs/ Head Offices /Zonal Offices/Global Link Services, Global IT Centre, foreign offices etc.) of State Bank of India, branches/other offices, Subsidiaries and Joint Ventures available at various locations and managed by the Bank (collectively referred to as **State Bank Group or 'SBG'** hereinafter). This Request for Proposal (RFP) has been issued by **the Bank** on behalf of **SBG** for hiring of Application Provider (AP) for END-TO-END SOLUTION FOR ANALYTICAL LAYER PLATFORM UNDER FRAUD RISK MANAGEMENT (FRM).

ii. In order to meet the Software ALP/ 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 ALP/ 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. Unless otherwise specifically permitted in Appendix-B, a bidder may not use the credentials of the original/parent entity of the bidder from which it has been demerged and come into existence, to meet the turnover, profit, experience or other eligibility criteria of 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 ALP/ 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.

3. DISCLAIMER

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

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

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

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

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

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

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

4. DEFINITIONS

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

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

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

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

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

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

vi. **"Vendor/Service Provider" or "Application Provider" or "AP"** 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.

vii. **Software Analytical Layer Platform/ Services/ System – "Software ALP" or "Services" or "System" or "ALP"** 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 ALP, such as installation, commissioning, implementation and integration with existing systems, provision of technical assistance, training, certifications, auditing and other obligation of Service Provider covered under the RFP.

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

ix. **“COTS”** - Commercial off-the-shelf product(s). Any product quoted shall be treated as Commercially available Off-The-Shelf (COTS) product if it meets the below requirements:

a. It is readily deployable with or without customization to suit the specific process requirements and does not involve developing the application from scratch or major significant developments in the product; and

b. It has been implemented by at least 8 organizations; and

c. It is implemented and maintained by at least 3 implementation partners other than the OEM of the COTS Software and each partner should have done at least one implementation. At least one of the implementation partners should have presence in INDIA.

x. **“Prototype”**: A prototype is an early sample, model, or release of a product built to test a concept or process. A prototype is generally used to evaluate a new design to enhance precision by business analysts and users. In this project, it will be expected that the AP will showcase a concept which will have the screens of the respective use cases and user shall be able to navigate from one screen to other to understand the business process flow.

xi. “**Days**”: All Working and Non-working days (365 days in a calendar year)

xii. “**Non-Working Days**”: 2nd and 4th Saturday of every month, Sundays and Public Holidays declared by the State Bank of India

xiii. **“Working Days”**: All other days except “Non-working Days”.

xiv. “**Concurrent use**r” connections are the number of concurrent user requests submission to the system at a point of time

xv. “**Go-Live**”: The system will be considered as “Live” based on the criteria defined in this RFP.

xvi. “**24*7**” is defined as three shifts of 8 hours every day. This is applicable for all seven days of the week without any non-working days

xvii. “**Scheduled Maintenance Time**” is defined as the time that the System is not in service due to a scheduled activity as defined in this SLA. The scheduled maintenance time would not be during the 16x7 (7:00 am to 11:00 pm) timeframe. Furthermore, scheduled maintenance time is planned downtime taken after permission of the SBI.

xviii. “**Scheduled operation time**” is defined as the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time. The total operation time for the systems and applications within the Primary DC, DR, will be 24x7x365 (per year).

xix. “**System or Application downtime**” is defined as the accumulated time during which the System is totally inoperable within the Scheduled Operation Time but outside the scheduled maintenance time. It is measured from the time a call is logged with the AP of the failure or the failure is known to the AP from the availability measurement tools to the time when the System is returned to proper operation.

xx. “**Availability**” refers to the time for which the services and facilities are available for conducting operations on the system including application and associated infrastructure. Availability is defined as: {(Scheduled Operation Time – System Downtime)/ (Scheduled Operation Time)} * 100%

xxi. “**Incident**” refers to any event/abnormalities in the functioning of the any of IT equipment/services that may lead to disruption in normal operations of the Data Centre, system or application services.

xxii. Terminologies utilized in this RFP are clarified in the following points

a. "System" as mentioned in this RFP refers to the ALP Application

b. "Administrator" as mentioned in this RFP refers to the "System Administrator"

5. SCOPE OF WORK

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

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

6. ELIGIBILITY AND TECHNICAL CRITERIA:

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

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

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

ii. The Bidder shall also submit **PRE-CONTRACT INTEGRITY PACT** along with technical Bid as prescribed in **Appendix-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.

7. COST OF BID DOCUMENT:

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

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

i. Bidder requiring any clarification on RFP may notify the Bank in writing strictly as per the format given in **Appendix-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.

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

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

9. CONTENTS OF BID DOCUMENT:

i. The Bidder must thoroughly study/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.

10. EARNEST MONEY DEPOSIT (EMD):

i. The Bidder shall furnish EMD for the amount and validity period mentioned in Schedule of Events of this RFP.

ii. EMD is required to protect the Bank against the risk of Bidder's conduct.

The EMD 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.

The 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.

iii. 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.

iv. The EMD of the unsuccessful Bidder(s) would be returned by the Bank within 2 weeks of the Bidder being notified as being unsuccessful.

v. 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.**

vi. No interest is payable on EMD.

vii. **The EMD may be forfeited: -**

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

(b) 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

(c) 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.

viii. If EMD is forfeited for any reasons mentioned above, the concerned Bidder may be debarred from participating in the RFPs floated by the Bank/this department, in future, as per sole discretion of the Bank.

11. BID PREPARATION AND SUBMISSION:

i. The Bid is to be submitted separately for technical and Price on portal of e-Procurement agency for **providing of** hiring of Application Provider (AP) for END-TO-END SOLUTION FOR ANALYTICAL LAYER PLATFORM UNDER FRAUD RISK MANAGEMENT (FRM) in response to the **RFP No. SBI:RMD/PRMD/2025-26/01** dated **02.01.2026.** Documents mentioned below are to be uploaded on portal of e-Procurement agency with digital signature of authorised signatory:

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

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

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

The scanned copy of original BG and tender fee demand draft should be uploaded subject to compliance of requirement mentioned in clause no 11"*DEADLINE FOR SUBMISSION OF BIDS*" sub-clause (ii).

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

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

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

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

(h) If applicable, scanned copy of duly stamped and signed Pre-Contract Integrity Pact subject to compliance of requirement mentioned in clause no 11"*DEADLINE FOR SUBMISSION OF BIDS*" sub-clause (ii).

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

(j) Certificate of Local Content as per Appendix _G__.

ii. **Price Bid for** providing of hiring of Application Provider (AP) for END-TO-END SOLUTION FOR ANALYTICAL LAYER PLATFORM UNDER FRAUD RISK MANAGEMENT (FRM) in response to the **RFP No. SBI:RMD/PRMD/2025-26/01** dated **02.01.2026** should contain only Price Bid strictly on the lines of **Appendix-F**. The 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 Price Bid) is received.

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

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

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

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

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

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

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

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

12. DEADLINE FOR SUBMISSION OF BIDS:

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

ii. Wherever applicable, the Bidder shall submit the original EMD Bank Guarantee, Tender Fees demand draft 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.

13. MODIFICATION AND WITHDRAWAL OF BIDS:

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

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

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

14. PERIOD OF BID VALIDITY AND VALIDITY OF PRICE Bid:

i. Bid (Technical and Price Bid) shall remain valid for duration of 6 calendar months from Bid submission date.

ii. 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.

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

15. BID INTEGRITY:

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

16. BIDDING PROCESS/OPENING OF TECHNICAL BIDS:

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

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

17. TECHNICAL EVALUATION:

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

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

18. EVALUATION OF PRICE BIDS AND FINALIZATION:

i. The Price Bid of only those Bidders, who are short-listed after technical evaluation, would be opened. The minimum qualifying score for being technically qualified would be < 70%> of the total technical score.

ii. After the opening of Price Bid, the scores of both Technical Evaluation and Commercial Evaluation would be calculated on 80: 20 basis (80% Weightage to Technical and 20% Weightage to Commercial)

iii. Successful bidder would be selected on the basis of Techno Commercial Evaluation as defined in Appendix-C.

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

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

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

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

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

19. CONTACTING THE BANK:

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

20. AWARD CRITERIA AND AWARD OF CONTRACT:

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

Guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order) and any revision thereto will be applicable for this RFP and 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.

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

ii. **Verification of local content**
The 'Class-I local supplier'/ 'Class-II local supplier' at the time of submission of bid shall be required to provide a certificate as per **Appendix-G** from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content requirement for 'Class-I local supplier'/ 'Class-II local supplier' as the case may be.

iii. Total cost of Software ALP 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 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 strictly on the lines of format given in appendix of this RFP, 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.

21. 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.

22. WAIVER OF RIGHTS:

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

23. CONTRACT AMENDMENT:

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

24. BANK’S RIGHT TO ACCEPT ANY BID AND TO REJECT ANY OR ALL BIDS:

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

25. BANK GUARANTEE:

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

ii. The Bank Guarantee is required to protect 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.

26. 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**.

27. SERVICES:

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

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

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

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

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 ALP. 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.

28. WARRANTY AND ANNUAL MAINTENANCE CONTRACT:

i. The selected Bidder shall support the Software ALP 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 ALP by State Bank of India.

ii. During the warranty and AMC period (if desired), Bidder will have to undertake comprehensive support of the Software ALP 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 ALP 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 ALP, 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 ALP and its components as per the Bank's requirements. Comprehensive maintenance shall include, among other things, day-to-day maintenance of the Software ALP as per the Bank's policy, reloading of firmware/software, compliance to security requirements, etc. when required or in the event of system crash/mal functioning, 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 ALP, Bidder shall ensure that Software ALP is made operational to the full satisfaction of the Bank within the given timelines.

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

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

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

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

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

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

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

29. PENALTIES:

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

30. 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.

31. 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/ ALP after delivery of the same to the Bank and where necessary reject the products/ALP which does not meet the specification provided by the Bank. This shall in no way be limited or waived by reason of the products/ ALP having previously being inspected, tested and passed by the Bank or its representative prior to the products/ ALP 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.

vi. The Bank reserve the right to appoint any third-party agency to conduct overall system implementation testing.

32. RIGHT TO AUDIT:

i. The Selected Bidder (Service Provider) shall be subject to annual audit by internal/ external Auditors appointed by the Bank/ inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ Software) and services etc. provided to the Bank and Service Provider is required to submit such certification by such Auditors to the Bank. Service Provider and or his / their outsourced agents / sub – contractors (if allowed by the Bank) shall facilitate the same The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by 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 grants unrestricted and effective access to a) data related to the outsourced activities; b) the relevant business premises of the service provider; subject to appropriate security protocols, for the purpose of effective oversight use by the Bank, their auditors, regulators and other relevant Competent Authorities, as authorised under law.

33. SUBCONTRACTING:

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

34. VALIDITY OF AGREEMENT:

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

35. LIMITATION OF LIABILITY:

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

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

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

a) claims that are the subject of indemnification pursuant to infringement of third party Intellectual Property Right;

b) damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider,

c) damage(s) occasioned by Service Provider for breach of Confidentiality Obligations,

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

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

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

36. CONFIDENTIALITY:

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

37. DELAY IN SERVICE PROVIDER'S PERFORMANCE:

i. Delivery, installation, commissioning of the Software ALP 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 ALP 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).

38. 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.

ix. Software Bill of Materials (SBOM)

All the software supplied to the Bank or developed for the Bank must be accompanied by a complete SBOM. The SBOM of the software supplied to the Bank or developed for the Bank must include the data fields contained in the **Appendix-R** of this document. In addition, the Software OEM/Owner/Vendor must ensure that:

- The Software supplied to the Bank or developed for the Bank is having a complete SBOM including all the dependencies up to the last level.
- Software OEM/Owner/Vendor should design a Vulnerability Exchange Document (VEX) after a vulnerability is discovered informing the bank about the exploitability status to help prioritize the remediation efforts.

  Subsequently, Software OEM/Owner/Vendor should provide the Common Security Advisory Framework (CSAF) advisory, which includes detailed information about the vulnerability, such as a description, affected product versions, severity assessment, recommended mitigation steps etc.
- Software OEM/Owner/Vendor will ensure update of the SBOM in case of any version update or any change in the details on the data point in the SBOM for any reason whatsoever.

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

39. 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 ALP 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.

40. INTELLECTUAL PROPERTY RIGHTS AND OWNERSHIP:

i. For any technology / Software / ALP developed/used/supplied by Service Provider for performing Services or licensing and implementing Software and ALP 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, non-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 ALP should be placed under an Escrow arrangement. All necessary documentation in this behalf should be made available to the Bank. In case of Escrow arrangement, complete details and the location and the terms and conditions applicable for escrow must be specified. Any update or upgrade to source code should be informed and brought under Escrow or made available to the Bank.

41. 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.

42. 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.

43. CODE OF INTEGRITY AND DEBARMENT/BANNING:

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

ii. Bidders are obliged under code of integrity to Suo-moto proactively declare any conflicts of interest (pre-existing or as and as soon as these arise at any stage) in

RFP process or execution of contract. Failure to do so would amount to violation of this code of integrity.

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

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

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

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

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

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

(e) **"Obstructive practice"** means materially impede the Bank's or Government agencies investigation into allegations of one or more of the above mentioned prohibited practices either by deliberately destroying, falsifying, altering; or by concealing of evidence material to the investigation; or by making false statements to investigators and/or by threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation; or by impeding the Bank's rights of audit or access to information;

v. **Debarment/Banning**

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

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

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

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

(b) Debarment from participation including removal from empanelled list

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

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

44. **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 ALP 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.

45. FORCE MAJEURE:

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

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

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

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

46. 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.

47. **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.

48. **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.

49. **GOVERNING LANGUAGE:**

The governing language shall be English.

50. **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.

51. 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.

52. 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.

53. 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.

54. 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.

55. **NOTICES:**

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

Part-II

Appendix–A

BID FORM (TECHNICAL BID)

[On Company’s letter head]
(To be included in Technical Bid)

Date: ______________

To:
< Address of tendering office >

Dear Sir,

Ref: RFP No. SBI:RMD/PRMD/2025-26/01 dated **02.01.2026**

~~~~~~

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, test, commission and support the desired Software ALP detailed in this RFP. We shall abide by the terms and conditions spelt out in the RFP. We shall participate and submit the commercial Bid through online auction to be conducted by the Bank’s authorized service provider, on the date advised to us.

i. While submitting this Bid, we certify that:

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

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

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

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

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

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

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

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 our acceptance thereof, would be binding contractual obligation on the Bank and us.

ix. 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.

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

xi. 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. We also certify that we have not been disqualified / debarred / terminated on account of poor or unsatisfactory performance and/or blacklisted by any Scheduled Commercial Bank / Public Sector Undertaking / State or Central Government or their Agencies / Departments at any time, during the last 3 years.

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

xiii. 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.

xiv. We hereby certify that on the date of submission of Bid, we do not have any major security incidents, data breaches, or cyber-attacks reported in relation to applications/ALPs deployed at client sites in Banking/Financial Services sector in past 5 years.

xv. We hereby certify that we have read the clauses contained in O.M. No. 6/18/2019-PPD, dated 23.07.2020 order (Public Procurement No. 1), order (Public Procurement No. 2) dated 23.07.2020 and order (Public Procurement No. 3) dated 24.07.2020 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.

xvi. If our Bid is accepted, we undertake to enter into and execute at our cost, when called upon by the Bank to do so, a contract in the prescribed form and we shall be solely responsible for the due performance of the contract.

xvii. We, 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 and amendment thereto		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. 200 crore during last 03 (three) financial year(s) i.e. FY’22-23, FY’23-24 and FY’24-25.		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	Bidder should have experience of minimum 5 years in providing the IT/ITES services		Copy of the order and / or Certificate of completion of the work. The Bidder should also furnish user acceptance report.

6	The Bidder (including its OEM, if any) should either be Class-I or Class-II local supplier as defined under this RFP.		Certificate of local content to be submitted as per **Appendix-G**.
7	Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India. (Start and End Date of the Project to be mentioned) in the past (At least 3 client references are required)		Bidder should specifically confirm on their letter head in this regard as per **Appendix-N**
8	Certification Requirements The Bidder should possess any three (3) of the below certifications which are valid at the time of bidding: i. ISO 9001:2008/ ISO 9001:2015 for Quality Management System ii. ISO 20000:2011 for IT Service Management iii. ISO 27001:2013 for Information Security Management System iv. CMMi Level 3 or above for Capability Maturity Model Integration v. PCI - DSS Note: The above certificate should be in the name of the Bidder		Copy of the Valid Certificate(s) to be provided
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 and also certify that they have not been disqualified /debarred /terminated on account of poor or unsatisfactory performance and/or blacklisted by any Scheduled Commercial Bank/ Public Sector Undertaking/ State or Central Government or their Agencies / Departments at any time, during the last 3 years.		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.
13	The Bidder/OEM should not have history in past 5 years from the date of RFP submission of major security		Bidder should specifically certify in **Appendix-A** in this regard.

	incidents, data breaches, or cyber-attacks reported in relation to applications/ALPs deployed at client sites in Banking/Financial Services sector		
14	Bidder / OEM should have implemented one of the following solutions in at least 2 banks with 2000 branches. Bidder's experience I. Enterprise vide Fraud Risk Management Solution II. AML/EWS III. Realtime transaction monitoring IV. Non-Realtime transaction monitoring V. Universal case manager		Bidder/ OEM has to submit the Purchase order/ Sign off/ Services Contract/ Go live mail/customer certificate clearly mentioning the services/ products and Satisfactory Performance Letter is also required from any one bank in which bidder is already engaged, concerned bank may use its own format for the purpose. Fraud monitoring/transaction monitoring should be mentioned on PO.
15	Bidder/OEM should have integrated experience in Transaction Monitoring System with minimum 5 channels out of following mentioned channels in single implementation: I. CBS II. Internet Banking III. Mobile Banking, IV. ATM V. E-commerce VI. UPI (Mandatory) VII. POS VIII. mATM IX. Debit Card		The letter of confirmation / confirmation mail from authorized signatory of such Bank mentioning one channel has to be provided. In case the letter only mentioned proposed solution is successfully running the same has to be substantiated by PO copy.
16	i The bidder should be either the Original Equipment Manufacturer (OEM)/ Original Software Developer (OSD) or their authorized representative in India. In cases where the manufacturer has submitted the bid, the bids of its authorized dealer will not be considered and EMD will be returned. And in case of		MAF to be submitted as per **Appendix - S**

	violations, both infringing bids will be rejected. ii If any product of Principal / Original Equipment Manufacturer (OEM) is being quoted in the tender, the OEM Company cannot bid for any other OEM's product. iii If an Indian Authorized Representative (IAR) submits bid on behalf of the Principal/OEM, the same IAR shall not submit a bid on behalf of another Principal/OEM		

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.

Name & Signature of authorised signatory

Seal of Company

Appendix-C

1. Technical Evaluation Matrix

S. No.	Criteria	Basis of evaluation	Max Marks	Supporting Evidence
A	**Bidder's Profile**		**15**	
A.1	The Bidder must have an average turnover of minimum Rs. 200 crores during last 03 (three) financial year(s) i.e. FY'22-23, FY'23-24 and FY'24-25.	i. Greater than or equal to Rs 500 Crores: 5 marks ii. Between 499 and 300 Crores: 3 marks iii. Between 299 Crores to 200 Crores: 1 mark (Turnover in Rs Crores)	**5**	Extracts from the audited Balance sheet and profit & Loss; OR Certificate from the statutory auditor
A.2	Bidder / OEM should have implemented one of the following solutions in at least 2 Banks with at least 2000 branches. Bidder's experience i Fraud Risk Management & Detection (FRMD) ii Real-time Transaction Monitoring iii Non-Real-time Transaction Monitoring iv Universal / Unified Case Manager v Device Fingerprinting / Behavioral Biometrics vi Mule Identification vii AI/ML-based Fraud or Risk Models viii Customer Peer Profiling, Device Profiling and Transaction Profiling ix Data Analytics Platform	Marks shall be allotted as given below: i. 5 banks = 10 Marks ii. 4 banks = 8 marks iii. 3 Banks = 6 Marks iv. 2 Banks = 4 Marks	**10**	Bidder/ OEM has to submit the Purchase order/ Sign off/ Services Contract/ Go live mail/customer certificate clearly mentioning the services/ products and Satisfactory Performance Letter is also required from any one bank in which bidder is already engaged, concerned bank may use its own format for the purpose. Fraud monitoring/transaction monitoring should be mentioned on PO.
B.	**Similar projects**		**35**	

B.1	Experience in Analytical Layer / platform and/or Fraud risk management solution and/ and/or projects of similar nature in BFSI sector for Development and/or COTS Implementation in India or Globally to be demonstrated in 5 Nos. engagements. The work order should have been issued within the last 5 years, as on Bid Submission Date.	i. equal to or more than 5 projects: 20 marks ii. 4 projects: 15 marks iii. 3 projects: 10 marks iv. 2 projects: 5 marks	**20**	Completion Certificates from the client; OR Work Order + Self Certificate of Completion (Certified by the Statutory Auditor); OR Work Order + Phase Completion Certificate (for Ongoing projects) from the client
B.2	Experience in developing, deploying and maintaining AI/ML Models for fraud prevention & Detection and/or in AML/EWS/ERM or related to similar nature in BFSI Sector in 5 number of Engagements within the last 5 years, as on Bid Submission Date.	i. equal to or more than 5 projects: 10 marks ii. 3 to 4 projects: 8 marks iii. 1 to 2 projects: 4 marks	**15**	Completion Certificates from the client; OR Work Order + Self Certificate of Completion (Certified by the Statutory Auditor); OR Work Order + Phase Completion Certificate (for Ongoing projects) from the client
C*	**ALP Proposed, Coverage & Methodology**		**200***	
C.1	Durability: Average transactions per day handled by the Analytical Layer / platform and/or Fraud risk management ALP and/or projects of similar nature deployed and live as on Bid submission date	Marks shall be allotted as given below: i. More than 30 Crore transactions per day = 10 Marks ii. Between 30 Crore to 20 Crore transactions per day = 8 Marks iii. Between 20 Crore to 10 Crore transactions per day = 6 Marks	**10**	Certificate from Client stating that ALP / solution has Transaction handling capacity

		iv. Less than 10 Crore transactions per day = 4 Marks		
C.2	Scalability: **Peak** transactions per second (TPS) handled by the Analytical Layer / platform and/or Fraud risk management ALP and/or projects of similar nature deployed and live in production environment as on Bid submission date	Marks shall be allotted as given below: i. More than 5000 = 10 Marks ii. Between 3500 to 4999 = 6 Marks iii. Between 3499 to 2000 = 4 Marks iv. Less than 1999 = 2 Marks	**10**	Client certificate confirming Peak TPS achieved in production 'or' performance / load test reports validated by client
C.3	Channel Integration Experience : Experience of integrating fraud and risk management / transaction monitoring solution with any 5 of the following channels **UPI is mandatory**, Core Banking Solution, ATM, E-Commerce, POS, Mobile Banking, Internet Banking, CBDC	2 marks for each channel integration	**10**	Client certificate or PO mentioning the channels and Go-Live state
C.4	ALP development methodology proposed for the demonstration of understanding of Software development and implementation, which would be required to deliver the service required by the Bank	Qualitative assessment based on Demonstration of understanding of the Bank's requirements through providing: i. ALP proposed and its components Technologies used ii. Scale of implementation iii. Learning on Issues iv. Challenges likely to be encountered v. Manpower resources plan post Go-Live vi. Mitigation proposed vii. Client references	**70**	To be showcased by the Bidder during Presentation

C 5	Live Demonstration and/or Site visit	Marks shall be allotted basis for the existing capabilities of the bidder as below: i FRMD Demo (rule engine and Case manager) = 20 Marks ii Unified Case Manager = 10 Marks iii Gen AI demo and utility including NLP / LLM for voice analytics and other use cases = 20 Marks iv ML Models for Network Graph Analysis / Mules and MLM frauds = 30 Marks v Self-serving / low-code no-code Dashboard environment = 10 mark vi SandBox & Rule Simulator capabilities = 10 mark	**100**	Live demonstration and/or Site visit

* 200 Marks will be adjusted to 50 as per the Indicative calculation as below:

a. Total Marks under section C = 200
b. Total Normalized marks for section C = 50
The indicative calculation is as below

Content	Max. Marks	Marks obtained by the Bidder
C1 - Durability	10	10
C2 – Scalability	10	10
C3 – Channel Integration Experience	10	10
C4 - ALP development methodology	70	40
C5 - Live Demonstration and/or Site visit	100	60
Total	200	130
Total Normalized Marks under section C	**50**	
Total Marks Obtained by the Bidder	= 130*(50/200) = 32.5	

2. Techno Commercial Evaluation:

Techno Commercial evaluation will be used for Procurement of Enterprise-Wide Analytical Layer Platform (ALP). The RFP shall specify the minimum qualifying score for the technical bid and also the relative weightages to be given to the technical criteria (quality) and cost.

1. The Criteria for Technical Evaluation and Commercial Evaluation will have weightage of **80:20**. Bidders scoring **less than 70% marks** in the Technical Evaluation will not be considered for the further selection process, and their Commercial Bids will not be opened.
2. The proposal with the Highest Weighted Combined Score (quality and cost / **TC1**) shall be selected.
3. 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 with a weight 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:

$$Combined\ Score\ of\ A = < 80 > x \frac{Technical\ Bid\ score\ of\ A}{Highest\ Technical\ Score} + < 20 > x \frac{Lowest\ Commercial\ Bid}{Commercial\ Bid\ of\ A}$$

III. 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.

S. 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).

IV. **Final Evaluation:** The commercials will be finalized among the shortlisted bidders who obtain <80>% 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 and Commercial score) and ranked TC-1 shall be recommended for award of contract. In case of a tie between bidders i.e. if two or more bidders receive the same combined score (‘S’), the bidder with the higher aggregate technical marks (t) shall be declared as successful bidder (TC – 1).

V. Kindly note that the Bank reserves the right to finalize the scores from the available bid documents and presentation made by the bidder and the Banks decision on techno commercial evaluation is FINAL.

Name & Signature of authorised signatory

Seal of Company

Appendix-D : Bidder Details

Bidder Details

Details of the Bidder

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

Name & Signature of authorised signatory

Seal of Company

Appendix-E : Scope of Work

Scope of Work and Payment Schedule

1. Description of Services:

1.1. Overview:

The purpose of this Request for Proposal (RFP) is to procure an Enterprise-Wide Analytical Layer Platform (ALP) to subsume the existing Proactive Risk management application.

The scope consists of Procurement for Supply, Implementation, Integration and Maintenance of the NextGen open, modular, secure, scalable & integrated END-TO-END SOLUTION FOR ANALYTICAL LAYER PLATFORM UNDER FRAUD RISK MANAGEMENT (FRM). This also includes maintenance & continuous support of the ALP. The operation and maintenance phase will be for a period of five (5) years after go-live of the system which can be further extended at the discretion of the Bank.

1.2. Background

The Proactive Risk Management (PRM) department is dedicated to overseeing and managing the bank's fraud risk, encompassing all aspects of prevention, detection, and timely response to fraudulent activities and safeguarding its customers. Operating 24/7, the department employs a PRM Application that generate alerts in both real-time (RT) and near real-time (NRT) modes, leveraging predefined business rules to swiftly identify and address suspicious transactions.

The Application is deployed in hybrid environment i.e. On-prem & Meghdoot cloud and it acts as a centralized platform for risk event handling, alerting, and case management. The Application supports rule-based configuration and MIS reporting, and it is integrated with auto dialer for customer verification.

Bank is now looking for a comprehensive Analytical layer Platform (ALP) to improve accuracy of fraud Prevention, Detection & Response and simultaneously reduce false positives and optimize & improve existing rules using analytical techniques to improve operational efficiency and reduce the rate of fraud in the Bank.

1.3. Scope of Work

The Analytical Layer Platform (ALP) is envisioned to transcend the scope of an enterprise fraud risk management. Beyond delivering all standard fraud-risk management functionalities, the ALP will act as a unified, centralized repository for comprehensive fraud-related data for one (1) year and few data segments applicable for effective fraud-risk management beyond (1) year, supporting a wide spectrum of fraud risk management operations. It will harness cutting-edge AI and machine learning models to enable sophisticated risk-based scoring, proactive fraud prevention, and real-time detection. The platform will incorporate specialized Mule and Scam detection models, advanced network and graph analytics for identifying complex fraud patterns, and AI/ML/NLP capabilities for voice data analysis. In addition, the ALP will provide interactive rule simulation tools, intuitive dashboards for insightful monitoring, and end-to-end workflow automation to streamline investigative and operational processes. This integrated, scalable, and intelligent ecosystem will empower SBI to enhance fraud risk mitigation with accuracy, agility, and efficiency. The scope of work includes the following:

1. Standard off the shelf Modules for Enterprise vide Fraud risk management solution including but not limited to Case Manager, Scenario / rule manager, Decision Engine, Rule simulator, Dashboarding platform, Enterprise reporting module, Data Sandbox, workflow management etc. customized as per the requirement of the Bank

2. Development of AI/ML models and advanced analytics module and related technologies

3. Supply of Manpower including data scientist and data engineers etc. post Go-live for continuous development and enhancement

The detailed scope of work is as follows

1.3.1. ALP Design, Development and Implementation:

I. Architect, Develop, Design and Integration of a Business and Technology Architecture solution for synergetic integration among multiple applications viz. Behavioral Biometrics, existing PRM application, Analytical Layer 2.0 and AI-Enabled Auto Dialer under a unified framework with Enterprise Architecture Alignment, optimization and strategic coherence.

II. The ALP should provide real-time and near real-time fraud detection across multiple banking channels including KIOSK, Retail and Corporate Internet Banking (RINB, CINB), Mobile Banking, UPI, ATM/POS, EPAY, CBDC, FasTag, YONO platforms, and foreign branches.

III. Enable ingestion, processing, and analytics on financial and non-financial transaction data from internal core banking systems, CRM, data warehouses, dialers, onboarding systems, etc. and external regulatory/intelligence data sources (DoT, RBI mule hunter, Indian Cyber Crime Coordination Centre, etc.).

IV. Ensure horizontal scalability to handle 22,000 peak transactions per second with sub-second response times for real-time detection.

V. Provide feature-rich ingestion pipelines supporting streaming and batch data processing modes with duplicate detection and data lineage tracking.

VI. Design and implement a scalable, high-throughput data analytics platform able to ingest diverse data types (structured, semi-structured, unstructured) from banking channels, core systems, third-party feeds, and regulatory sources.

VII. Develop ETL pipelines supporting real-time, near real-time, and batch processing with change data capture (CDC) and data validation.

VIII. Maintain a centralized data lake, operational data store (ODS), enterprise data warehouse (EDW), and specialized data marts optimized for fraud analytics.

IX. Implement data cleansing, enrichment, de-duplication, and metadata management consistent with GoI data governance best practices.

X. Deliver master data management (MDM) with golden record consolidation for customers, accounts, and transactions.

XI. Integrate any interface/API already developed/procured by Bank with the ALP.

1.3.2. Data Reservoir, Lake, and Analytical Data Marts

I. Provide scalable distributed storage architecture for structured, semi-structured, and unstructured raw data with fault tolerance and schema-on-read capability.

II. Maintain immutable raw data with WORM storage capabilities, point-in-time snapshots, and time-travel functionality for investigation reproducibility.

III. Design and implement curated enterprise data lake and analytics marts including dimensional fraud-specific models, customer and transaction behavior analytics, risk assessment marts, dashboards & reporting requirements.

IV. Maintain metadata cataloging, data lineage visualization, and data provisioning pipelines enabling real-time and batch data flow.

V. Provide role-based, column-level access controls and encryption for all data stores.

1.3.3. Data Quality, Validation, Conditioning and Governance

I. Implement comprehensive data validation rules covering schema adherence, referential integrity, completeness, null handling, duplicate detection, and statistical anomaly detection.

II. Enrich ingested data with customer demographics, merchant risk classifications, and external intelligence overlays.

III. Facilitate data standardization including timestamp normalization, currency and numeric formatting, and address normalization.

IV. Execute privacy protection including automated PII detection, masking/tokenization, role-based dynamic data access, audit logs, and compliance to domestic and international privacy laws (DPDP, GDPR).

V. Implement backup, disaster recovery, high availability, and business continuity plans adhering to Bank’s IT policies.

1.3.4. Self-service Secure Data Sandbox for Advanced Analytics

I. Create an isolated, secure sandbox environment that enables data scientists and fraud analysts to develop, test, and validate new fraud patterns & scenarios.

II. Provide containerized workspaces equipped with popular data science languages (Python, R, Scala, SQL) and collaborative IDEs (Jupyter, RStudio).

III. Implement synthetic data generation, differential privacy, and automatic PII scanning to maintain data confidentiality.

IV. Support advanced simulation techniques including Monte Carlo and agent-based modeling.

V. Enable synthetic data generation and drift monitoring capabilities.

VI. Provide experiment tracking, version control, model explainability frameworks (SHAP, LIME), and governance workflows including model promotion to production.

1.3.5. Intelligence and Analytics Engine

I. Deliver a comprehensive fraud detection engine incorporating:

a. Rule-based fraud detection with rule management, testing simulators, versioning, and governance.

b. AI/ML capabilities including supervised and unsupervised models, ensemble methods, deep learning, and graph neural networks for pattern recognition.

c. Real-time risk scoring combining behavioral, device, network, and external data.

d. Graph network analysis for entity linkage, mule detection, community detection, and money laundering rings.

e. Natural Language Processing (NLP) model including complaint sentiment analysis, entity extraction, and multilingual support.

f. Voice analytics for customer-analyst conversations with emotion and sentiment detection.

II. Support model lifecycle management with continuous training, drift detection, threshold optimization, and explainable AI features ensuring regulatory compliance.

III. Implement false positive reduction engines using machine learning for rules implemented in the system

IV. Provide adaptive scoring and threshold management with multi-dimensional risk calibration.

V. Integrate external intelligence feeds, DoT MNRL List, DoT Fraud Risk Indicators, Mule Hunter.ai, i4C Suspect registry, DPIP, watchlists, sanctions, and blacklists with versioning and audit trails.

1.3.6. Behavioral Profiling and Scoring

I. Establish baseline behavioral profiles for every customer, employee, device.

II. Capture behavioral biometrics such as typing cadence, mouse movement, gesture rhythm, OTP entry speed, and device orientation.

III. Monitor login frequency, session length, transaction velocity, navigation flow changes, and payee behavior changes.

IV. Implement geolocation profiling, detect spoofing, impossible travel, and cross-device/shared device risks.

V. Maintain unified Behavioral Risk Scores combining behavioral, device, and geolocation risk indicators.

VI. Provide API interfaces for real-time Behavioral Risk Score consumption and alerts generation.

1.3.7. Channel Specific Monitoring, Mule, SCAM Detection

I. Implement specialized profiling and detection models for cards, channels, UPI transactions, and branch/remote banking.

II. Monitor non-financial events for early fraud indicators (PIN changes, address modifications, balance inquiries).

III. Detect mule accounts, circular fund transfers, beneficiary hopping, and transaction clustering across channels.

IV. Set dynamic limits and automated actions for suspected mule accounts.

V. Provide channel-specific fraud typology detection including refund abuse, contactless bursts, mass beneficiary uploads, and maker-checker bypass attempts.

VI. Incorporate Telecom sector signals (SIM swap, roaming) and IP reputation for enhanced risk assessment.

VII. Support multi-channel case intake, classification, lifecycle management, and escalation workflows configurable per fraud typology.

VIII. Integrate AI-powered case prioritization, routing, and workload balancing.

IX. Provide centralized, secure repositories for documentation and communication with full audit logging.

X. Enable configurable notifications, dashboards, and management reporting with trend and predictive analytics.

1.3.8. MIS, Reporting and Dashboards

I. Provide self-service, low-code/no-code BI platforms for users across business, investigative, administrative, executive roles, fraud analysts, operations, and management with rich visualization options (charts, heat maps, KPIs).

II. Deliver diverse visualizations (charts, heat maps, KPI cards) and support multi-dimensional slicing and drill-through capabilities.

III. Build role-based dashboards optimized for fraud analysts, supervisors, call centers, business analysts, and executives.

IV. Include performance management dashboards tracking analyst productivity, model accuracy, rule effectiveness, and system performance.

V. Support ad-hoc investigation reporting, historical case analytics, and operational MIS reports.

VI. Provide audit-ready documentation and secure historical report repositories.

VII. Support multi-language localization and seamless integration with CRM, case management, and workflow orchestration systems.

VIII. Enable multi-dimensional analysis, drill-down, and ad hoc query support.

IX. Deliver standardized reports for regulatory compliance and operational oversight.

X. Support report distribution workflows and integration with CRM and case systems.

1.3.9. Testing Environment and Rule Simulator

I. Provide a comprehensive, fully integrated testing environment with rolling historical data for rule simulation. This must be a dynamic environment to replicate real and / or production environment

II. Enable parallel testing and performance benchmarking of multiple rules with real-time impact analysis on alerts and false positives.

III. Implement comprehensive parameter management, change tracking with maker-checker workflows, version control, and rollback capabilities.

IV. Support simulations of threshold sensitivity and non-monetary event rules (address change, device changes, PIN resets).

V. Provide logical and arithmetic expression builders for scenario creation.

VI. Support both real-time and batch rule execution with analysis of execution success.

1.3.10. Alerting and Scoring Framework

I. Deliver real-time and batch scoring infrastructure with latency below 100ms capable of processing Maximum 22,000 TPS with a provision for year-on-year enhancement.

II. Perform multi-level entity scoring (transaction, customer, network) with composite risk aggregation.

III. Implement advanced clustering algorithms (k-means, hierarchical, DBSCAN, graph-based) etc. for fraud pattern discovery.

IV. Support alert prioritization, suppression of false positives, intelligent routing between dialer and analyst, duplicate alert reduction, and alert grouping into consolidated actionable events.

V. Integrate communication gateways for email, SMS, WhatsApp, dialer systems, voice Bots etc. for alert notifications.

VI. Maintain audit trails for all alert and case actions.

VII. Provide network visualization of alert relationships with interactive graphs and collaboration features.

1.3.11. Workflow Automation

I. Provide end-to-end workflow management from alert generation to case closure with full audit trails and dynamic role-based access.

II. Enable multi-user workflow participation with collaboration, escalation management, and conflict resolution.

III. Support maker-checker authorizations on critical actions, change approvals, and emergency workflows.

IV. Integrate with CRM, dialers, communication gateways, and case management for seamless investigator workflows.

V. Provide scheduling and duty management for call analysts including shift rotations, leave management, and real-time adjustments.

1.3.12. Support, Maintenance and Training

I. Provide 24x7 onsite and remote support for the analytical layer and integrated channels with defined SLAs.

II. Provide desired manpower like Data scientist, Data Engineers & MLOps Engineers post-go-live for new model development, enhancements and BI dashboards.

III. Conduct periodic training sessions for Bank staff on administration, usage, and analytics capabilities.

IV. Support patch management, upgrade implementation, compliance with security policies, and audit recommendations.

V. Facilitate disaster recovery drills and provide capacity and health monitoring of the overall analytics platform.

1.3.13. Security and Compliance

I. Comply with Bank's IT and Information Security Policies including encryption standards, access controls, and regulatory guidelines.

II. Ensure robust data privacy protection in line with DPDP, GDPR, PCI-DSS, and RBI master directions.

III. Integrate with Bank's SOC tools including but not limited to SIEM,DAM PAM, PIMS, AV, and DLP etc. for centralized monitoring.

IV. Conduct regular vulnerability assessments, penetration testing, and ensure remediation tracking.

V. Maintain incident response readiness and participate in periodic security audits by Bank and regulators.

VI. The detailed requirements are available in **Appendix T.**

VII. Integration with Bank's Resilience operation center (ROC).

2. Description of Deliverables

The Application Provider (AP) will be responsible for delivering the following items for the Analytical Layer Platform as per the detailed description below:

S. No.	Stage	Deliverable	Description
1	Stage -1	Resource Deployment at Location, Project Plan	Contract signoff, Team deployment at location and project plan to be provided / provisioned by the AP
		SRS, TRS & Technical Design documents	AP to assess the BRD and prepare and submit the SRS document, Technical Architecture & Sizing requirements
		Infrastructure Readiness and Environment Readiness for Development, production, pre-prod, UAT	Assess the hardware and infrastructure readiness (servers, network, storage, resources) Prepare detailed installation procedures and checklists for software, hardware, and middleware components for all environment i.e Development, production, pre-prod, UAT and / or testing
		Installation, Planning and Preparation of ALP & Provide off the shelf licenses	Install software applications, databases, tools, and licenses according to project standards Conduct configuration of system parameters, network settings, user access controls, and security mechanisms & Validate installation against baseline configurations
2	Stage - 2	Data Integration framework and Ingestion - Phase 1	Integration with Channels, CBS, Datawarehouse, PRM Application & Dialer and Ingest data from these sources. Provision of APIs, connectors, and message queues for seamless integration
3	Stage 3	Deployment of Core Analytics: • Case Management • Rule Management • Reporting & Dashboard • Rule Simulator, Test Environment and SandBox • Decision Engine • User Access Management • Alert Management	Full-featured case management including workflow and escalation. Migration and enhancement of existing business rules with centralized management and versioning. Development of comprehensive rule simulation and testing capabilities Complete migration of all reporting and dashboard functionalities as well as development of reports as per functional Specification

			Synthetic data generation functionality for rule testing and Data sandbox
4	Stage 4	Data Integration framework and Ingestion - Phase 2	Integration with Behavior biometric solution, CRM, AML & on-boarding channels as well as external source integration like DoT MNRL, FRI, i4C suspect registry, RBI Mule hunter & CFR repository, NCRP portal etc.
5	Stage 5	Development & Customization of Advanced Analytics • AI-Based transaction scoring model • Scam detection • Mule Detection • Anomaly detection • False positive reduction • Network / Link & Graph analysis	Development and deployment of AI/ML models for fraud detection and scoring Implementation of advanced network and graph analytics capabilities Development and deployment of False positive, Scam & mule detection (Mule hunter shall be leveraged) Deployment of risk scoring models integrated with analytics
6	Stage 6	Peripheral Requirements • Offline Transaction Monitoring (OTMS) / AML-CFT integration • AI Model for voice call analysis of analyst • Design specific workflows for operations, OTMS and Admin • integration of proposed ALP with the Bank's current security and operations management systems like SOC, PIMS, DLP, AD, ITAM, Centralized Key Management System, etc. as per **Appendix 'T'**	Offline Transaction Monitoring System (OTMS): A comprehensive module designed to analyze historical transaction data in for detecting fraudulent patterns and suspicion in branches. AI Model for Voice Call Analysis of Analysts: An advanced artificial intelligence ALP that processes and analyzes voice call data between analysts and customers. This model leverages natural language processing (NLP) and speech analytics to detect anomalies, sentiment, compliance adherence, and conversation quality. Design of Specific Workflows for Operations, OTMS, and Administration Development and implementation of tailored, role-specific workflows that streamline fraud risk management operations, offline transaction monitoring activities, and administrative processes.

			Integration with Bank’s Security and Operations Management Systems: Seamless integration of the proposed analytical ALP with the bank’s existing security and operational infrastructure, including but not limited to: • Security Operations Center (SOC) for centralized security monitoring and incident response. • Privileged Identity Management System (PIMS) for controlled access to sensitive resources. • Data Loss Prevention (DLP) for safeguarding critical data. • Active Directory (AD) for authentication and user management. • IT Asset Management (ITAM) systems for tracking and managing IT assets. • Centralized Key Management System for encryption key lifecycle management. • Network Automation (NA) tools to orchestrate network security policies. The detailed security requirements are available in **Appendix ‘T’**
7	Stage 7	User training, SOPs, User-guides, ALP testing & Go-Live & O & M Phase	• Successful Go Live of ALP the production environment.

The detailed description of deliverables is as below:

2.1. Requirement Finalization, Project Plan & Infrastructure Assessment

The AP should validate, provide and finalize the BRD, SRS, Project plan and infrastructure assessment and requirement as per the description below:

2.1.1. Requirement finalization along with validation of BRD and SRS

a. The AP must perform a detailed assessment of the business and ALP as described in this RFP. Based on the AP’s comprehension and individual assessment, the AP shall develop and finalize the Business Requirements Document (BRD) and System Requirement Specifications (SRS) in consultation with the SBI and its representatives. Whilst doing so, the AP is expected to perform the following.

b. In case of any changes in the indicative Functional Requirement Specification of the application as attached with this RFP, the SBI will provide the modified information to the AP. The AP shall study and revalidate these with the SBI at the time of construction and accordingly submit an exhaustive BRD & SRS document.

c. The AP shall organize multiple workshops during the requirement gathering stage of each phase. This is important for the AP to validate the to be design and incorporate the user feedback in the ALP Application requirement and design.

d. The AP shall develop and follow standardized templates for requirements capturing and system documentation.

e. The AP must maintain a traceability matrix from the SRS stage for the entire implementation.

f. The AP must receive sign off from user groups formed by the SBI.

g. For all discussions with the SBI team, few team members of the AP shall always be present at the SBI office (Jaipur & Mumbai).

h. The templates for all the deliverables shall be finalized with the SBI.

2.1.2. Project Plan

i. Application Provider shall develop a High-Level Project Plan, in collaboration with SBI within 1 month of the effective date as defined in the Master Service Agreement that shall describe how all the elements of project management work together to ensure that scope and schedule are being managed holistically.

j. Application Provider shall develop detailed Project Plan for each implementation phase separately.

    a. Description of the application Vendor’s organization with their proposed staffing, roles, and responsibilities.

    b. Project organization and communication structure.

    c. Processes and tool sets to be used for project management, quality assurance, risk management, problem resolution, and other areas Application Provider deems relevant and important to the successful management of the Project.

k. Project plans and schedules giving details of schedule of various tasks and subtasks, task durations, dependencies, deliverables, milestones, resource deployment, meetings and information required from SBI.

l. Resource planning and deployment, indicating where resource would be based during that phase, i.e. onsite at SBI premises or offsite at Application Provider premises.

m. During the project implementation, Application Provider shall provide regular reports to SBI on the results accomplished during the period report to SBI, on following items (weekly/fortnightly/monthly templates):

n. The Project Plan will be updated every quarter in consultation with SBI.

o. Application Provider shall be responsible for maintenance of a Requirement Traceability Matrix to demonstrate compliance with requirements and specifications as mentioned in the RFP. The Requirements Traceability Matrix would be a live document throughout the project, and Application Provider team should update the document to reflect the compliance at every stage.

2.1.3. Infrastructure Requirements Assessment

a. Infrastructure will be provided by SBI, and it is clarified to the Application provider that he should liaison with infrastructure provider to provision for the Data Centre (DC), & Data Recovery Center (DR) for hosting the IT Infrastructure. The Application providers are required to carefully assess the requirements specified in this RFP and size the infrastructure accordingly. Application providers are free to propose any higher / additional infrastructure that may be required as per their proposed ALP to meet the project requirements, its scope of work and SLAs as listed in this RFP.

b. Application Provider shall perform the detailed assessment of ALP requirements and assess the infrastructure requirements (including servers, storage, networking, security etc.) and liaison with Infrastructure provider for operationalization of the ALP and providing the services in conformance with the SLA described in the RFP.

c. Application Provider shall be responsible for sizing the hardware and ensure that infrastructure provisioned shall support the scalability and performance requirements of the ALP. The Application Provider shall ensure that the servers are sized adequately and redundancy towards high availability of all components is built into the architecture by infrastructure provider and meets the requirements of service levels as mentioned in the RFP.

d. The proposed ALP should meet the requirements of functionality, performance, security, scalability, and availability of the ALP.

e. Application Provider shall liaison with the service providers for providing necessary IT infrastructure and applications at the existing Data Centers as per the requirements.

f. It is expected that Application Provider shall design a ALP which would optimize the space and power requirements at the data centers.

g. DR site will be provided so that all the business-critical data is available at all times. In case of invocation of the DR site, all business-critical system should be available for use. The following modules (excluding functional dependencies on other modules) may be considered as business-critical systems:

h. Application Provider shall design the ALP and liaison with infrastructure service provider in the Bank to ensure RTO (Recovery Time Objective) of less than 15 mins and RPO of near real time

i. It is expected that Application Provider shall design a ALP which would optimize the license requirements without compromising the quality of delivery

j. In case, AP propose COTS ALP as part of ALP application, then the AP will be responsible for supplying the application and perpetual licenses of related software products and installing these to meet the ALP requirements.

k. The AP shall perform periodic audits to measure the license compliance against the number of valid end user software licenses consistent with the terms and conditions of license agreements, volume purchase agreements and other mutually agreed upon licensed software terms and conditions. The AP shall report any exceptions to license terms and conditions at the right time to SBI. However, the responsibility of license compliance solely lies with the AP. Any financial penalty imposed on the SBI during the contract period due to license non-compliance shall be borne by the AP.

2.2. Integration with Digital channels, SBI Applications and external sources

The Application provider shall ensure the integration and/or data ingestion with various sources as below:

Channels*	Internal Sources*
CARD	Core Banking (CBS)
CBDC	DataWarehouse
CINB_MERC	Existing PRM Application
CINB	Dialer
CMP	Behavior Biometric solution
EPAY	On-boarding channels
FASTAG	CRM/AML/KYC/OTMS
FO	Communication Gateways (e-mail, SMS, WhatsApp)
KIOSK	**External Sources***
MERC	DoT (MNRL list)

MOB	DoT Fraud Risk Indicator (FRI)
RINB	DPIP
UPI	I4C Suspect Registry & NCRP data
YONO	RBI Mule Hunter & CFR list
YONO2	NPCI

* It shall be noted that the list is indicative, covering majority of the touchpoints, the final list shall be provided by the Bank to the Application Provider at the time of AP on-boarding.

2.3. Development/Customization of ALP Tracks

The Application Provider (AP) shall supply, install, design, customize, integrate and implement the proposed Analytical Layer Platform (ALP) in a modular, track-based manner aligned to the Bank’s fraud-risk management needs and the stages defined in this RFP. This shall include, at a minimum, the following activities:

2.3.1. Functional and Technical Design

2.3.1.1. The AP shall prepare detailed Functional Design and Technical Design in line with the overall Technical Architecture & Sizing finalized under Stage-1, ensuring reuse of common components (data models, features, rules, scoring engines, APIs, dashboards) and alignment with the Bank’s enterprise data and security architecture.

2.3.1.2. The AP shall design track-specific configurations (rules, parameters, thresholds, workflows, queues, dashboards etc.) to support both real-time (RT) and near real-time (NRT) use-cases as applicable.

2.3.1.3. The AP shall configure out-of-the-box capabilities of the proposed ALP wherever feasible and shall undertake customization only where mandatory requirements cannot be met by configuration.

2.3.1.4. All track-specific logic (rules, parameters, scenarios, lists, routing, SLAs) shall be implemented in a parameterized manner so that they are changeable by authorised Bank users without code changes, to the extent supported by the product.

2.3.1.5. Customizations shall conform to secure coding practices, Bank’s S-SDLC requirements and cyber-security requirements defined in this RFP (including **Appendix ‘T’**).

2.3.1.6. Each ALP track shall be designed to consume data from the common Data Integration Framework and Ingestion layers (Stage-2 and Stage-4), as well as from the Core Analytics components (Stage-3), without point-to-point or ad-hoc integrations.

2.3.1.7. The AP shall ensure that all tracks use standardized interfaces, shared data models and common services (e.g. scoring, alerting, case management, reporting, sandbox, rule simulator) to avoid duplication and to facilitate maintainability and scalability.

2.3.1.8. For tracks requiring AI/ML-based models (e.g. transaction scoring, mule detection, scam detection, anomaly detection, false positive reduction, OTMS, voice call analysis), the AP shall design and develop the necessary features, models and integration hooks in coordination with the activities under Stage-5 and Stage-6.

2.3.1.9. Behavioural profiling, network/graph analytics, external intelligence integration (DoT, i4C, RBI Mule Hunter, DPIP, etc.) and OTMS requirements shall be embedded into relevant tracks as per **Appendix-E-1** and **Appendix-E-2.**

2.3.1.10. For each track, the AP shall ensure availability of required configurations, data sets and test cases in the development, SIT, UAT, Rule Simulator and Data Sandbox environments, in line with Section 2.4 (ALP Software Testing) and the Testing Environment & Rule Simulator requirements in **Appendix-E-1.**

2.3.1.11. The AP shall support SBI and its designated agencies in conducting end-to-end testing of each track (functional, integration, performance, security, parallel-run comparisons with existing PRM) and shall address defects, gaps and optimization requirements without additional cost.

2.3.1.12. The AP shall prepare and maintain track-wise documentation, including detailed configuration guides, run-books, parameter catalogues, rule and model inventories, data mappings and operational procedures, as an integral part of Development/Customization.

2.3.1.13. The AP shall ensure that all artefacts produced as part of track development/customization (designs, configuration scripts, code, test cases, results, SOPs) are version-controlled and handed over to the Bank as per the documentation and exit management requirements of this RFP

2.3.1.14. All Development/Customization of ALP Tracks shall be carried out in accordance with the overall project plan and stage-wise timelines defined in **Appendix-E,** and in full compliance with the Bank's IT, Information Security, Data Governance, S-SDLC and regulatory requirements.

2.4. ALP Software Testing

a. The AP shall conduct independent testing (including Unit Testing, Functional Testing, Integration Testing, Security Testing, Performance Testing etc.) before deployment of the developed Integrated ALP Application at DC/DR.

b. The AP shall thoroughly test the performance of ALP Application for proper load/ concurrent users.

c. The AP shall ensure that for each module & features developed for ALP Application is tested.

d. The AP shall prepare & share the testing documents (covering Test Strategy, Test Cases & Test results) and standards with the SBI and any designated third-party auditor (TPA), wherever applicable/ required.

e. The AP shall assist the SBI & its designated authority in successful completion of User Acceptance Testing (UAT) of the developed modules & features of ALP Application on the completion of the development work for each phase.

f. The SBI may appoint Third Party Agency (TPA) at its own cost to conduct the technical reviews and audits of development work performed by the AP.

g. SBI & its designated authority/ TPA (if any) shall conduct functional, security & performance testing of the deployed ALP Application for each Phase.

h. The AP shall be responsible for:

h.1. Preparation and submission of Test Strategy, test cases and Test Results

h.2. Demonstration of module-wise functionalities/ features to SBI & its designated authority/ TPA (if any) after deploying the ALP Application at DC/DR for each Phase.

h.3. Support SBI & its designated authority/ TPA (if any) for conducting the testing, audits etc. and provide access of the systems as required by them.

h.4. Coordination with the cert-in vendor appointed by SBI and assist SBI in obtaining the safe-to-host certification (if applicable).

h.5. Rectification in the ALP Application for any issues/ bugs/ improvements/ enhancements/ upgradations suggested by SBI & its designated authority/ TPA (if any) during the UAT at No additional cost.

h.6. Removal of all vulnerabilities/ security threats identified during the testing done for safe-to-host/ UAT/ technical audit/ testing, etc. by SBI & its designated authority/ TPA (if any) at No additional cost.

h.7. Submit the report/ testing documents including details of defects/ bugs/ errors found and corrective actions taken.

h.8. The AP shall obtain sign-off from the SBI on the UAT for each Phase of ALP Application after successful implementation of all the changes/ recommendations received from SBI & its designated authority/ TPA (if any).

2.5. Go-Live of Software ALP

Only after the UAT sign-off for all modules by the SBI, the deployed ALP Application would be deemed commissioned.

a. The AP shall provide below-mentioned documents for all modules & features covered in respective phase of application development.

b. Installation Manuals

I. User Manuals (Role wise)

II. Access Control Policy

III. System administrator manuals

IV. Toolkit guides and troubleshooting guides

V. Source code library

c. After the successful commissioning of all modules of the ALP Application, the ALP application would be declared as Go-Live.

d. After the Go-live of ALP Application, the AP will start providing O&M services for 5 years as per the agreed SLA.

e. SBI will be responsible for providing the infrastructure & network connectivity to the AP for running the ALP Application. SBI will identify the internet service provider (ISP) & Infrastructure Service Provider for this purpose at its own cost.

f. The AP will:

I. Facilitate, integrate and provide all technical support to the SBI to get required network connectivity and monitor the uptime of network connectivity/ link in coordination with DC/DR operator.

II. Record & manage the database for IT assets like hardware, system software, application software and COTS products etc. deployed for ALP Application at DC/DR, by recording the information like configuration details, Licenses, Version Numbers and Registration

2.6. Training and capacity building

a. The AP shall ensure proper hands-on training to the team of selected trainers & end-users designated by SBI on the software ALP developed by Application provider so as to make them well conversant with all the functionalities, features and processes built in the ALP Application.

b. Training shall be conducted either at SBI offices or any other location identified by SBI. Training may be divided into multiple sessions as per the need and requirement of the project/ application.

c. The AP in consultation with SBI shall conduct Training Needs Analysis of all the staff concerned during system study phase and drawing up a systematic training plan.

d. To meet the training requirement for successful implementation of project, the Application provider shall perform following activities (but not limited to) in consultation with SBI:

I. Prepare a training plan and submit it to respective stakeholders.

II. Design the Training session with sufficient training duration for meaningful assimilation of training content by an average user.

III. There should be sufficient number of trainers (at least 2) in every training session for conducting the training program.

IV. Provide a training material (role base) and the language of training material shall be in Hindi and English. The AP shall ensure that all the training documentation in Hardcopy and Softcopy is in place (user training, operation procedures, visual help-kit etc.).

V. Propose different training modules for different user profiles at appropriate timelines as modules go live in production.

e. Conduct the training to the designated staff and technical team.

I. SBI shall identify respective officers/ staff involved in various business areas. The AP shall provide training of identified officers/ staff.

II. The requisite training infrastructure like training space, computers, projector with screen, and connectivity to Server shall be provided by SBI

2.7. Data migration from existing Application & server

a. The AP shall prepare a plan of action for smooth migration of data from existing database and PRM application to ALP.

b. The AP shall ensure 100% accuracy in the migrated data. In case any correction is identified by SBI in the migrated data, the same shall be corrected by the AP.

c. The AP shall submit a MIS Report to designated authority of SBI indicating amount of data migrated.

2.7.1. Parallel Run, Data Sanctity and Migration

The Bank intends to introduce the new Analytical Layer in a phased manner and run it in **parallel** with the existing PRM application before full cut-over. The bidder shall propose and implement a comprehensive parallel run strategy covering:

2.7.1.1. Validate functional equivalence or improvement of the new solution vis-à-vis current PRM rules and alerting.

2.7.1.2. Compare alerts, risk scores, and decisions (approve/decline/suppress) across channels and products.

2.7.1.3. Establish accuracy, stability, and performance benchmarks before decommissioning the current PRM.

2.7.1.4. Propose a **phased parallel run plan**, including minimum recommended duration for each phase (e.g., pilot, controlled expansion, full-volume parallel).

2.7.1.5. Each phase shall specify scope (channels/rule sets/models), data volumes, KPIs, and exit criteria.

2.7.1.6. The Bank reserves the right to extend or shorten phases based on observed performance.

2.7.1.7. The parallel run shall at minimum cover all critical channels currently monitored in PRM (e.g., UPI, Cards, RINB, CINB, YONO/YONO Lite, KIOSK, Fastag, EPAY, CBDC, etc.). High-risk and high-volume rule sets in RT and NRT regimes.

2.7.1.8. The existing PRM application shall remain the **system of record** and **system of decision** for all RT/NRT fraud decisions and blocking actions until formal cut-over.

2.7.1.9. The new Analytical Layer shall operate in **shadow mode** (no customer-impacting decisions) during initial phases, generating risk scores and alerts for comparison.

2.7.1.10. A clearly defined mechanism shall be provided to compare Transactions evaluated, Rules triggered, Alerts generated Decisions recommended vs. PRM decisions

2.7.1.11. The bidder shall define, track, and report on KPIs agreed with the Bank, including but not limited to Detection rate / strike rate by channel, rule and fraud type, Latency of RT / NRT decisioning versus current PRM SLAs and Stability and error rates of interfaces and pipelines

2.7.1.12. Exit criteria for each phase of the parallel run and for final cut-over must be clearly defined and agreed with the Bank.

2.7.2. Data Sanctity, Validation and Reconciliation

2.7.2.1. The bidder shall be responsible for ensuring data sanctity across all stages of ingestion, processing, storage and consumption within the new Analytical Layer, and for matching results produced during parallel run and post-migration.

2.7.2.2. At a minimum, the solution and bidder’s approach shall include the End-to-End Data Consistency with mechanisms to ensure that all transactions ingested into PRM are also ingested into the Analytical Layer during parallel run, including RT/NRT event flows and associated enrichment data (e.g., CBS, EIS, channel parameters).

2.7.2.3. Validation rules at ingestion and processing stages (e.g., format, range, referential checks, mandatory fields). Automatic error handling, quarantining of bad records, and re-processing capabilities. Generation of data quality reports for each pipeline, including completeness, timeliness, duplicates, and error rates.

2.7.2.4. Provide automated or semi-automated reconciliation mechanisms to match records between Source systems (channels, CBS, DWH/Data Lake, CRM, PRM) and the Analytical Layer and Old PRM data structures and new Analytical Layer data structures, including RT/NRT records and alert histories.

2.7.2.5. Any discrepancies shall be logged with clear exception reasons and reported to the Bank on agreed frequency

2.7.2.6. Maintain **full data lineage** from source to consumption layers, including transformations applied.

2.7.2.7. Comprehensive audit logs for data loads, rule/model execution, user actions, configuration changes, and migrations.

2.7.3. Data Migration and Cut-Over Plan

2.7.3.1. The bidder shall propose and execute a comprehensive Data Migration and Cut-Over Plan from the existing PRM application and related data sources to the new Analytical Layer.

2.7.3.2. The plan shall cover the historical transaction data required for models, profiling, and analytics (beyond current 90-day retention, leveraging DWH/Data Lake where applicable).

2.7.3.3. Historical PRM data including RT and NRT transaction records Alerts, cases, dispositions, and analyst actions Blocking/unblocking events and autodialer outcomes etc.

2.7.3.4. Detailed migration approach (e.g., bulk load from DWH/Data Lake, incremental loads, CDC where applicable).

2.7.3.5. Staged migration with clear cut-off dates for each data category.

2.7.3.6. Use of staging and validation environments prior to loading into production data structures.

2.7.3.7. Rollback strategy in case of failure or significant mismatch.

2.7.3.8. Detailed data mapping document between existing PRM schemas and the new Analytical Layer’s data model (including RT/NRT tables, alert/case tables).

2.7.3.9. Business rules and transformations applied during migration (e.g., field standardization, code mapping, enrichment logic).

2.7.3.10. Clear treatment of duplicate, inconsistent, or obsolete data.

2.7.3.11. Pre-migration and post-migration reconciliation reports (record counts, hash totals, key value comparisons).

2.7.3.12. Sampling and detailed validation procedures for critical entities (high-risk customers, confirmed fraud cases, mule accounts, etc.).

2.7.3.13. Formal sign-off criteria for each migration batch and for overall migration completeness and correctness.

2.7.3.14. Cut-Over Strategy should include detailed cut-over plan from parallel run to full production usage of the Analytical Layer, including: Final cut-off time for PRM as decision engine, Switch-over of RT/NRT decisioning from PRM to the new solution

2.7.3.15. Documentation and Knowledge Transfer of migration design, scripts, configurations, reconciliation procedures, and cut-over steps. Knowledge transfer sessions for Bank’s PRMD, IT-RA, Analytics and Operations teams to enable independent execution of future migrations or backfills if required.

2.8. Operations and maintenance for five (5) years after Go-Live including IT helpdesk support for the SBI users

a. Bidder shall provide requisite skilled and qualified resources onsite from the OEM during the implementation and integration period.

b. The AP shall deploy the O&M Team onsite from the start of O&M period till the end of contract period.

c. The proposed services shall be normally manned for a period of 24/7 hours as per the requirement throughout the year or as decided by SBI. But in exceptional condition or in urgency of work, the support might be required on holidays. The AP shall maintain an attendance register for the resources deployed.

d. Also, it would be the responsibility of the AP to retain the deployed for the entire Contract/ Project duration or in the event of a resource leaving employment with the AP, the same shall be immediately replaced with another resource of equivalent or higher qualifications and experience of resource leaving employment with the AP. All such events should be notified prior to SBI in writing and should be in accordance with the SLAs mentioned in this RFP.

e. The staff provided by the AP will perform their duties in accordance with the instructions given by the designated officers of SBI from time to time. SBI will examine the qualification, experience etc. of the personnel provided before they are put on the designated positions. The AP has to take approval from SBI for the proposed staff before their deployment. SBI has every right to reject the personnel, if the same is not acceptable, before or after commencement of the awarded work/ project.

f. It is responsibility of the AP to scale up the Operations & Maintenance (O&M) team as and when required to confirm smooth execution throughout the duration.

g. The Bidder shall provide additional count of skilled and qualified L1 and L2/L3 resources, in the future if the Bank decides, at the same terms and rate during the contract period.

h. The bidder should inform 1 month in advance and obtain concurrence from bank if they want to replace the dedicated resource with the equivalent or better one.

i. Bidder must maintain and test BCP Plan periodically for providing resources to Bank & services in any disruptive scenario.

j. Bidder shall provide the Information & Cyber security training and Privacy training to its resources before deputing in the Bank.

k. Bidder shall perform the Due Diligence of all subcontractors engaged for the activity and shall share with the Bank.

l. Onsite support should be available 24*7 for the proposed ALP.

m. Bidder should train the resources who will be deployed before onboarding.

n. **Scope of Work for Level One (L1) Support**

I. L1 would typically address queries and all end user issues pertaining to: Business application related issues/queries, Enterprise applications (In-Scope), Generic IT Queries, Queries related to business process, reports generation, presentation layer applications, etc. and Other environmental software related to the ALP solution.

II. The Bank reserves the right to increase or decrease the number of seats at L1 helpdesk depending on its requirements. The Bank also reserves the right to change the locations of helpdesks at its discretion. The Bidder should also note that the setup at the L1 helpdesk must provide for 1 supervisor and/or 1 support personnel from the Bank.

III. The Bank expects the Bidder to provide for L1 support for all activities and services that are part of scope.

IV. The key activities that the bidder is expected to perform as part of Level 1 Helpdesk Support are:

1. User Management
2. Creation or modification of user profiles
3. Assessment in case of specific rights assignment

4. Provision for assigning user rights only for certain fixed period

V. Periodic user right monitoring (at known frequency) must be specified and implemented

VI. Categorization of requests into functional clarification, bug or change request.

VII. Functional clarification / work around to be provided by Level 1 support itself.

VIII. Bug change requests to be logged and reported for further processing

IX. Provide telephonic and / or electronic mechanisms for problem reporting requests as well as for service and status updates.

o. **Scope of Work for Level Two (L2) Support**

I. The Bank expects the Bidder to provide L2 support for all activities and services that are part of the scope.

II. The L2 support provided by the Bidder should be comprehensive and cover entire management and support of all the ALPs provided by the Bidder (ALP and all third-party ALPs). The services specified herein are not exhaustive and only indicative.

III. Provide continuous onsite support for all the applications being implemented and being procured through the bidder

IV. Troubleshoot online processing or batch processing activity at various levels in the ALP

V. Troubleshoot any query processing activity at various levels in the ALP

VI. Resolve the call within stipulated timeframe as defined in Service Level Agreement

VII. Coordinate with the L3 teams for resolution and provide necessary information as may be required by the team to resolve the issues

VIII. Escalate the unresolved calls as per escalation matrix Automatically log in calls during escalation

IX. Provide the timeframe for providing a ALP of resolution of the escalated calls

X. Prepare a root cause analysis document with the resolutions provided for major issues such as:

XI. Production issues

1. Problems which have resulted in complete service disruptions or downtime
2. Delayed response times
3. Data / table corruptions
4. System Performance issues (high utilization levels)

XII. Liaise with the L1 support personnel for the call information and resolution.

XIII. All other activities as would be required by the Bidder to manage and maintain the ALPs.

XIV. Perform the application audit on a quarterly basis or as mutually agreed with the bank.

XV. Rectify any corruption in the software.

XVI. Ensure patch releases are ported to the production environment with no business disruption or business losses.

XVII. Support BCP/DR drills.

XVIII. The resources shall be responsible for creating/configure and customize the ALP as per Bank’s requirement.

XIX. Provide application support from the Bank's data center as mentioned above for the Data center and disaster recovery site.

XX. Routing the transactions through the backup system in case the primary system fails

XXI. Support for integrating any applications that need to be interfaced with the ALP in the future.

XXII. Level 2 service desk agents would need to be deployed by the bidder at DC/DR premise from where the Level 2 support is planned to be provided. The bidder is expected to act upon the tickets routed from Level 1. The bidder has to ensure that proficient and professional personnel are put to handle the L2 support and resolutions are provided on a proactive basis.

XXIII. The L2 helpdesk resources proposed should have adequate and relevant experience in the areas mentioned like database and ALPS application. The Bank has a right to review and reject resources whose competency levels are below expectations. Support and maintain all interfaces to the ALPS and other ALPs part of this scope document modifications to existing scripts, reports presentation to Bank management on the critical issues reported, resolved, ALP provided and the suggested recommendations or leading practices as and when asked by the Bank or on a monthly basis whichever is earlier. Perform performance tuning of the applications mentioned in the Scope of Work of this document including ALP tuning.

p. Scope of Work for Level Three (L3) Support

I. Critical code level changes or application software related issues. This support is required for all components that are expected to be provided by the Bidder as part of this RFP.

II. The Bidder has to provide the resolution / service as per the defined service levels in this RFP. The Bidder has to make sure that the methodology proposed for addressing and resolving problems is aligned to the required and defined service levels.

III. The Bidder should staff the service desk with persons who are conversant with the ALPs deployed and are capable of resolving routine problems and queries through the service desk application or over the phone. The staffing needs of the service desk will be decided by bank based on calls/ticket volumes and patterns.

IV. Brief description of the envisaged activities to be performed by Bidder at L3 is enumerated as under. The services specified herein are not exhaustive and are only indicative:

1. Resolve the call within the stipulated timeframe as defined under the service level agreements.

2. Communicate the status of the call to the Bank and accordingly update the status, ALP or workaround and date of resolution.

3. Prepare a root cause analysis document for issues referred to L3 support and provide to the Bank along with the resolution.

4. Liaise with the L2 support personnel for the call information and resolution.

5. Provide version upgrades for ALPS application.

6. The resources shall be responsible to close the audit gaps, if found in the third party audit report shared by the Bank during the entire contract period.

7. The L3 resource shall be responsible for proactively closing the vulnerabilities and Internal Information System's Audit observations related to the ALPS system to make the system resilient to cyber threats in the mentioned TAT defined by the Bank.

8. L3 support shall be responsible for Patching of the system with the latest patches available.

9. All other activities as would be required by the SI to manage and maintain the ALPs.

10. Perform Version Migration - The services specified herein are not exhaustive and only indicative.

11. Perform version migration as per the version release plan of OEM and agreed by the Bank.

12. Version upgrades and migrations should also include porting of existing customizations.

13. Provide training to the Bank's core functional and technical team members on the new version functionalities and technical aspects as and when version upgrades and migrations are performed. For any version migration to be performed, the Bank and the bidder will mutually draw up an implementation plan and schedule for the same.

2.9. Software Bill of Materials (SBOM)

a. As part of RBI Advisory on Software Bill Of Materials (SBOM), the selected bidder has to identify & submit SBOM for the application / product, including direct dependency & transit dependency.

b. Selected bidder shall capture & develop detailed ALP Design that includes Security measures, Network segmentation, Identity and access management, Bill of Materials (BOM, SBOM, CBOM), Architecture, Metrics and operational considerations.

c. The bidder shall abide by the guidance on Software Bill Of Materials provided by SBI to the selected bidder.

2.10. Documentation

The Bidder shall provide the detailed documents including but not limited to the following:

a. Detailed SRS (System Requirement Specifications) Document
b. High Level Architecture Document
c. Techno - Functional Risks and Mitigation Document Functionality Traceability matrix which would provide details on the interdependence of the technical components for the realization of functionality. This matrix should provide a projection of the efforts required for completion of a technical module.
d. High Level Design Document
e. Low Level Design Document
f. Data Flow Diagrams
g. Test Plans
h. Comprehensive Test Cases Document (Unit, Integration and UAT Test Cases tested)
i. Deployment Plan Document
j. Content Management Guide
k. Change Management Methodology Document Security Guide
l. User Management Guide
m. Release Notes

3. Term of the Project - Project Schedule, Milestones, Delivery Locations and Payment Schedule

a. The initial contract period shall be five years (5) years from the date of completion of Stage 7 i.e. Go-live of complete ALP with the possibility of an extension at the sole discretion of the Bank, on mutually agreed terms and conditions, including pricing.

b. If the Bank does not terminate the contract at the end of the initial five-year period, the contract shall automatically extend for an additional 1 years on mutually agreed terms and conditions, including pricing.

c. Kindly note that the timelines in this section are indicative and once the project commences, the AP will be responsible for preparing the project charter & PERT chart which will cover a detailed project plan, high level communication plan, project risk, and approach as per the scope under this RFP.

d. The project needs to be completed as per agreed timelines and project plan for the scope of the work mentioned in the RFP. The delay due to non-provision of hardware, software, infrastructure services or any delay which are not attributable to the Application provider will not be considered.

e. It is expected that the key project manager & Team to be based in the SBI PRM premises at Jaipur, Corporate Centre, Mumbai and GITC, Navi Mumbai wherever required, and the project team can scale up and down based on the intensity of the delivery.

The SBI will be providing the necessary IT infrastructure (Hardware) and hosting facilities for the ALP. The AP will be required to provide infra sizing considering the KPIs, data points and system requirements.

f. Indicative Timelines & Activities:

T = Release of Purchase Order to the Application Provider (AP)

Miles tone	Stage	Deliverable	Timelines (In Weeks)
1	Stage -1	Resource Deployment at Location, Project Plan SRS, TRS & Technical Design documents Infrastructure Readiness Installation, Planning and Preparation of ALP & Provide off the shelf licenses	T + 4
2	Stage - 2	Data Integration framework and Ingestion - Phase 1	T+8
3	Stage - 3	Deployment of Core Analytics Modules: • Case Management • Rule Management • Enterprise Reporting & Dashboard • Rule Simulator & Testing Environment • User Access Management • Alert Management	T+16
4	Stage - 4	Data Integration framework and Ingestion - Phase 2	T+18
5	Stage – 5	Development & Customization of Advanced Analytics module • AI-Based transaction scoring model • Scam detection • Mule Detection • Anomaly detection • False positive reduction • Network / Link & Graph analysis	T+20
6	Stage - 6	Peripheral Requirements • Offline Transaction Monitoring (OTMS) • AI Model for voice call analysis of Customers	T+22

		• Design specific workflows for operations, OTMS and Admin • integration of proposed ALP with the Bank’s current security and operations management systems like SIEM, DAM, SOC, PIMS, DLP, AD, ITAM, Centralized Key Management System, NA	
7	Stage - 7	User training, SOPs, User-guides, ALP testing & Go-Live	T+24
8	Stage - 8	Operation & Maintenance	Go Live + 5 Years

4. Payment Schedule

Miles tone	Stage	Deliverable	Payment Schedule
Payment Schedule during Implementation Phase till Go-Live			
1	Stage -1	Resource Deployment at Location, Project Plan SRS, TRS & Technical Design documents Infrastructure Readiness Installation, Planning and Preparation of ALP & Provide off the shelf licenses	On completion of stage 1 - 5% of the Total Implementation cost
2	Stage - 2	Data Integration framework and Ingestion - Phase 1: Integration with Channels, CBS, Datawarehouse, PRM Application & Dialer and Ingest data from these sources. Provision of APIs, connectors, and message queues for seamless integration.	On completion of stage 2 – 10% of the Total Implementation cost
3	Stage - 3	Deployment of Core Analytics Modules: • Case Management • Rule Management • Enterprise Reporting & Dashboard • Rule Simulator & Testing Environment • User Access Management • Alert Management	On completion of stage 3 – 10% of the Total Implementation cost
4	Stage - 4	Data Integration framework and Ingestion - Phase 2: Integration with Behavior biometric solution, CRM, AML & on-boarding channels as well as external source integration like DoT MNRL, FRI, i4C suspect registry, RBI Mule hunter & CFR repository, NCRP portal.	On completion of stage 4 – 10% of the Total Implementation cost
5	Stage – 5	Development & Customization of Advanced Analytics module • AI-Based transaction scoring model • Scam detection • Mule Detection • Anomaly detection • False positive reduction • Network / Link & Graph analysis	On completion of stage 5 – 10%% of the Total Implementation cost
6	Stage - 6	Peripheral Requirements	On completion of stage 6

		• Offline Transaction Monitoring (OTMS) • AI Model for voice call analysis of Customers • Design specific workflows for operations, OTMS and Admin • integration of proposed ALP with the Bank's current security and operations management systems like SOC, PIMS, DLP, AD, ITAM, Centralized Key Management System, NA	– 10% of the Total Implementation cost
7	Stage - 7	User training, SOPs, User-guides, ALP testing & Go-Live & UAT Signoff	On completion of stage 7 – 45%% of the Total Implementation cost
Payment Schedule Post Go-Live			
8	ATS	ATS support will start Post Go-Live	Quarterly in arrear, at the end of each quarter
9	Manpower Support	Technical Manpower Support Post Go-Live	Quarterly in arrear, at the end of each quarter

Note

1. For the purpose of this Payment Schedule, The Implementation Cost is defined as the total cost of Table '**A**' & Table '**B**' of **Appendix F** – Price Bid

2. The Payment is subject to the completion of successful Stages and the Penalty if any as defined under **Appendix J**

Appendix E-1: Functional Specification

1 Data Ingestion: from Existing Channels

Sr. No.	Requirement ID	Requirement Description	Mandatory (M) / Desirable (D)*	Compliance (Yes/No) and Supporting Documents	Available as part of ALP (Yes / No)	Will be Provide as Customization (Yes / No)	Will be provided as Third Party ALP	Feasible (Yes/No)
1	DI-CH-001	The Solution shall ingest all financial and non-financial transactions and events from existing Bank channels, including but not limited to Cards, ATM, RINB, CINB, CINB_MERC, YONO, YONO2, MOB, MERC, EPAY, CBDC, KIOSK, FasTag, CMP and UPI, into the PRM Analytical Layer.	M					
2	DI-CH-002	The Solution shall ingest both debit and credit transactions for all supported channels	M					
3	DI-CH-003	The Solution shall ingest financial transactions (for example, payments, transfers, withdrawals, deposits, refunds) and non-financial events (for example, logins, balance enquiries, PIN/credential changes, profile changes, device registrations, OTP requests, card/account status changes), wherever such data is available from the channel or its integration system.	M					
4	DI-CH-004	For Bank-designated real-time channels (such as UPI, Cards/ATM, RINB, CINB, YONO, EPAY, MOB), the Solution shall ingest events in real time	M					

		such that they are available for scoring and analytics within the latency bounds defined in the Performance & Scalability section of this RFP.						
5	DI-CH-005	For Bank-designated near-real-time or batch channels (such as KIOSK, FasTag, CMP and other NRT feeds), the Solution shall ingest events in near real time (for example, in micro-batches) such that they are available for analytics within the latency bounds defined in the Performance & Scalability section of this RFP.	M					
6	DI-CH-006	The Solution shall be able to ingest channel-specific event attributes (for example, ATM terminal/location, POS merchant details, UPI VPA, QR code details, merchant category, device identifiers, session IDs) as provided by each channel, for use in fraud analytics and profiling.	M					
7	DI-CH-007	The Solution shall support the onboarding of new Bank channels or new message types in future (for example, new digital products) by reusing the common ingestion framework and data model, without requiring architectural redesign of the ingestion layer.	M					
8	DI-CH-008	The Solution shall support ingestion of non-financial behavioural /clickstream data from digital channels (for example, YONO, RINB, CINB, MOB), where made available by the Bank, for use in behavioural and session-level fraud analytics.	M					

2 Data Ingestion: from Bank’s existing Core Banking, Datawarehouse, CRM, Dialer, PRM Application, OTMS, Onboarding Data & Analytics Data lake

Sr. No.	Requirement ID	Requirement Description	Mandatory (M) / Desirable (D)	Compliance (Yes/No) and Supporting Documents	Available as part of ALP (Yes / No)	Will be Provide as Customization (Yes / No)	Will be provided as Third Party ALP	Feasible (Yes/No)
9	DI-INT-001	The Solution shall ingest customer and account master data (for example, CIF, account numbers, product types, status, opening/closing dates, branch, segment) from the Core Banking System (CBS) and/or Enterprise Data Warehouse/Data Lake, at a frequency agreed with the Bank (for example, daily or more frequent).	M					
10	DI-INT-002	The Solution shall ingest historical and ongoing credit and debit transaction data from the Bank’s Data Warehouse/Data Lake, sufficient to support fraud analytics, behaviour profiling and model training, with the minimum historical horizon 12 months specified by the Bank.	M					
11	DI-INT-003	The Solution shall ingest CRM data, including at least customer complaints and service requests related to digital transactions, fraud disputes, and their outcomes (for example, resolved, rejected, chargeback), at a frequency	M					

		defined by the Bank, for use in rule/model development and feedback loops.						
12	DI-INT-004	The Solution shall ingest Dialer and contact-centre interaction logs related to PRM alerts (for example, call attempts, call results, customer response), including where available call disposition codes and timestamps, for use in outcome analysis and model training.	M					
13	DI-INT-005	The Solution shall ingest data from the existing PRM application, including at least: rules (identifiers and versions), alerts generated, alert outcomes (for example, genuine, suspected, confirmed fraud), actions taken (for example, blocks, whitelists) and case references.	M					
14	DI-INT-006	The Solution shall ingest onboarding, KYC and risk flag data (for example, customer risk category, EWS/AML flags, PEP status, blacklist/negative list indicators) from relevant onboarding and AML/KYC systems, at a frequency defined by the Bank, for use in fraud risk profiling.	D					
15	DI-INT-007	The Solution shall ingest relevant data from the Bank’s existing Analytics Data Lake (for example, vulnerability scores, other analytical scores/models agreed by the Bank) and make such scores available as features for the PRM Analytical Layer.	M					

16	DI-INT-008	Where call recordings or transcripts are made available by the Bank from Dialer or contact-centre systems, the Solution shall be able to ingest associated metadata (for example, call IDs, timestamps, customer identifiers) and link them to alerts/cases for NLP or voice analytics by other components of the Solution.	D					
17	DI-INT-009	The Solution shall support the linkage of records across CBS, CRM, PRM, channel systems and Data Warehouse/Data Lake using stable identifiers (for example, CIF, account number, mobile number, email), to provide a unified customer and entity view for fraud analytics.	M					
18	DI-INT-10	The Solution shall be able to ingest new internal datasets that the Bank may identify in future (for example, new internal risk scores, new operational systems), using the common ingestion framework and without architectural redesign of the ingestion layer.	D					
19	DI-INT-11	The solution should integrate & configure OTMS (Offline transaction monitoring system) Rules for Branch and / or staff transactions and / or In-operative accounts / surge accounts financial and non-financial transactions and support future configuration	M					

3 Data Ingestion: External Regulatory and Intelligence Data Sources

Sr. No.	Requirement ID	Requirement Description	Mandatory (M) / Desirable (D)	Compliance (Yes/No) and Supporting Documents	Available as part of ALP (Yes / No)	Will be Provide as Customization (Yes / No)	Will be provided as Third Party ALP	Feasible (Yes/No)
20	DI-EXT-001	The Solution shall ingest data from Department of Telecommunications (DoT) sources, including at least Mobile Number Registry (MNRL) and Fraud Risk Indicator (FRI) datasets made available to the Bank, at frequencies agreed with the Bank, for use in fraud detection and profiling.	M					
21	DI-EXT-002	The Solution shall ingest i4C Suspect Registry and NCRP (National Cyber Crime Reporting Portal) data provided to the Bank, with configurable synchronization frequency, and make these records available for rule and model building	M					
22	DI-EXT-003	The Solution shall ingest RBI-related fraud intelligence, including RBI Mule Hunter outputs and Central Fraud Registry (CFR) data, as these are provided to the Bank, and make them available for entity risk profiling and mule	M					

		detection within the PRM Analytical Layer.						
23	DI-EXT-004	The Solution shall be prepared to ingest data from DPIP (Digital Payments Intelligence Platform) or similar future regulatory /intelligence platforms, as and when such data becomes available to the Bank, using the common ingestion framework and without architectural redesign.	M					
24	DI-EXT-005	The Solution shall support ingestion of third-party fraud intelligence and sanctions/watchlist datasets. Negative list, blacklist etc.and make these available for screening and risk scoring within the PRM Analytical Layer.	M					
25	DI-EXT-006	The Solution shall support configurable refresh frequencies for each external source (real time, hourly, daily, weekly), as agreed with the Bank, and shall apply the same validation, error handling and lineage controls defined in ‘Data Ingestion Common Requirements’.	M					
26	DI-EXT-007	The Solution shall support a secure fallback mechanism for manual ingestion of external datasets (for example, via secure portal upload or SFTP) when automated integration is temporarily unavailable, ensuring that such manually ingested data passes through the same	D					

		validation and lineage controls as automated feeds.						
27	DI-EXT-008	The Solution shall support matching of Bank customers, accounts, devices and transactions against external lists and intelligence datasets using deterministic keys (for example, PAN, mobile number, account) and configurable fuzzy matching (for example, name, address), and shall expose a match score or confidence level for each hit.	M					
28	DI-EXT-009	The Solution shall support full versioning and historical retention of external lists (suspect registries, sanctions lists) such that the Bank can, for any past decision, identify which version of a list was in effect at that time.	D					
29	DI-EXT-010	The Solution shall support the onboarding of additional regulator-mandated or third-party external sources in future using the common ingestion framework, without architectural redesign of the ingestion layer.	D					

4 Data Ingestion Common Requirements

Sr. No.	Requirement ID	Requirement Description	Mandatory (M) / Desirable (D)	Compliance (Yes/No) and Supporting Documents	Available as part of ALP (Yes / No)	Will be Provide as Customization (Yes / No)	Will be provided as Third Party ALP	Feasible (Yes/ No)
30	DI-COM-001	The Solution shall support data ingestion from all configured sources (channels, internal systems and external sources) using one or more of the following mechanisms, as required by the Bank: REST / webhooks, message bus (for example, Kafka or equivalent), AMQP/JMS queues, SFTP file transfer, gRPC or similar protocols, and database Change Data Capture (CDC).	M					
31	DI-COM-002	The Solution shall support ingestion of data in JSON, XML, CSV and fixed-width formats and, where applicable, standard financial message formats such as ISO 8583 / ISO 20022, as used by the Bank.	M					
32	DI-COM-003	The Solution shall allow changes in source file or message layouts (for example, addition of non-mandatory fields, changes in field order) to be handled via configuration or mapping definitions, without requiring changes to the core ingestion engine code,	D					

		wherever the underlying technology supports such configurability.						
33	DI-COM-004	The Solution shall detect and handle duplicate records/events from any source based on configurable keys (for example, transaction ID, account, customer ID, external reference, timestamp window), ensuring that duplicates are not processed twice for scoring/analytics unless explicitly configured, and shall log the deduplication decision and reason.	M					
34	DI-COM-005	For each configured source, the Solution shall validate at least: data types, field lengths and presence of mandatory fields. Records failing validation shall be routed to an error queue or quarantine with an error code and description and shall not be used for scoring/analytics until corrected or re-ingested.	M					
35	DI-COM-006	The Solution shall support configurable business-rule checks on ingested data (for example, valid date formats, non-negative amounts where applicable, valid codes and identifiers), and shall flag or reject records that violate these checks, with reasons logged for each rejected record.	D					

36	DI-COM-007	The Solution shall generate ingestion reconciliation summaries per source (channel, internal system, or external provider) for a given period, showing at minimum: total records received, total successfully ingested, total failed/errored, and total duplicates suppressed, so that the Bank can verify ingestion completeness.	M					
37	DI-COM-008	The Solution shall maintain data lineage such that, for any record used in the PRM Analytical Layer, the Bank can identify the originating source system/provider, the ingestion date/time, and the ingestion mechanism (for example, API, file, queue, CDC), and can distinguish raw/landing data from curated/processed data.	D					
38	DI-COM-009	The Solution shall provide an ingestion operations view (for example, dashboard or standard reports) displaying, per source: current ingestion status, volume received over a selected period and count of validation errors, with information refreshed at a configurable short interval as agreed with the Bank.	D					

39	DI-COM-010	The Solution shall generate operational alerts to a monitoring console and/or via email/SMS, when ingestion for any configured source stops or falls below a configurable threshold, or when validation/error counts for a source exceed configurable thresholds, so that the Bank can take timely corrective action.	M					
40	DI-COM-011	During or immediately after ingestion, the Solution shall standardize timestamps to Indian Standard Time (IST) while retaining original source time zone as metadata and shall ensure that text data is stored using a consistent character encoding (for example, UTF-8) across all ingestion sources, unless otherwise required by the Bank.	D					
41	DI-COM-012	The Solution shall allow authorized Bank users to pause, resume and, where appropriate, reprocess specific ingestion feeds (for example, selected files, topics, or time windows) via a controlled interface, with all such actions recorded in an audit trail for later review.	M					
42	DI-COM-013	The Solution should be designed so that adding a new source (channel, internal system, or external provider) reuses the same common ingestion components, monitoring, error handling and data quality controls,	M					

		without requiring architectural redesign of the ingestion layer.						

5 AI/ML Models & Intelligence

Sr. No.	Requirement ID	Requirement Description	Mandatory (M) / Desirable (D)	Compliance (Yes/No) and Supporting Documents	Available as part of ALP (Yes / No)	Will be Provide as Customization (Yes / No)	Will be provided as Third Party ALP	Feasible (Yes/No)
43	FR-AM-01	The solution shall support multiple model types for fraud detection, including supervised (e.g., tree-based, gradient boosting, neural nets) and unsupervised (e.g., clustering, isolation forests, autoencoders) methods.	M					
44	FR-AM-02	The solution shall support graph/network analytics (e.g., entity linkage, community detection, graph embeddings) for detecting mule networks, MLM/pyramid and ring-based frauds.	M					
45	FR-AM-03	The solution shall compute unified, real-time risk scores at transaction and entity level using ensembles of rules and models, with sub-second scoring for high-risk channels.	M					

46	FR-AM-04	The solution shall support feature engineering on financial and non-financial data (behaviour, devices, locations, relationships) and maintain a reusable feature store.	M					
47	FR-AM-05	The solution shall support model training and evaluation using labelled historical data, with standard metrics (e.g., precision, recall, F1, AUC-ROC) and segment-wise performance.	M					
48	FR-AM-06	The solution shall provide model explainability (e.g., SHAP, LIME or equivalent) and human-readable reason codes for scores/alerts.	M					
49	FR-AM-07	The solution shall support threshold configuration and optimization (per channel/product/segment) using historical performance and “what-if” analysis.	M					
50	FR-AM-08	The solution shall support MLOps capabilities: model versioning, CI/CD-style deployment to staging/production, champion-challenger testing and rollback.	M					
51	FR-AM-09	The solution shall monitor model and rule performance over time (volumes, hit rates, precision/recall, drift in data	M					

		and features) and raise alerts on degradation.						
52	FR-AM-10	The solution shall support periodic and on-demand model retraining using recent data, with approval workflows before promoting new models. It should also train basis the feedback loop on the actions taken by the analysts	M					
53	FR-AM-11	The solution shall support use of the Bank’s own AI/ML models alongside built-in models, using a common scoring framework.	M					
54	FR-AM-12	The solution shall support continuous learning from feedback (case outcomes, investigator labels) to improve models/rules and reduce false positives over time.	M					
55	FR-AM-13	The solution shall support NLP techniques (e.g., NER, classification) on unstructured text such as complaints, call transcripts, and case notes for fraud signals.	M					
56	FR-AM-14	The solution shall support human-in-the-loop controls, allowing analysts to override model decisions with captured reasons and feed this back into model improvement processes.	M					

57	FR-AM-15	The solution shall maintain a model registry with metadata (version, training data period, features used, performance metrics) for audit and regulatory reviews.	M					
58	FR-AM-16	Maintain a library of configurable fraud detection model templates for rapid deployment and adaptation.	M					
59	FR-AM-17	Provide scalable, parallel model deployment with champion-challenger frameworks and resource management.	D					
60	FR-AM-18	Implement advanced graph/network analytics for fraud pattern recognition with real-time relationship mapping.	M					
61	FR-AM-19	Enable flexible dynamic thresholds with automated tuning and A/B testing to optimize detection rates and reduce false positives.	D					
62	FR-AM-20	Ensure ethical AI deployment with safety controls including human-in-the-loop overrides and LLM safety guardrails.	D					

6 Channel Specific Analytics

Sr. No.	Requirement ID	Requirement Description	Mandatory (M) / Desirable (D)	Compliance (Yes/No) and Supporting Documents	Available as part of ALP (Yes / No)	Will be Pro vide as Customizat ion (Yes / No)	Will be provide d as Third Party ALP	Feasi ble (Yes/ No)
63	FR-CA-01	The solution shall support detailed card analytics including spending patterns, MCC risk, preferred ATMs/merchants, card-present and CNP fraud typologies (e.g., small-value testing, rapid country/merchant switching, refund abuse, contactless bursts).	M					
64	FR-CA-02	The solution shall support ATM/POS analytics for both financial and non-financial events (withdrawals, deposits, PIN changes, balance inquiries, reversals) to detect preparatory and active fraud patterns.	M					
65	FR-CA-03	The solution shall support comprehensive UPI analytics (P2P, P2M, M2P) including behavioral profiling of customer, device, IP, VPA, beneficiaries, QR usage and typical UPI typologies (spam collect, mandate abuse, rapid new beneficiary payouts, beneficiary hopping).	M					
66	FR-CA-04	The solution shall support location and session-based analytics (e.g., IP geolocation, impossible travel, VPN/proxy detection,	M					

		high-risk domains, high-risk geographies) across online channels.						
67	FR-CA-05	The solution shall support analytics for fund-transfer patterns across channels (UPI/IMPS/NEFT/RTGS/cards/wallets/YONO), including velocity, burst patterns, circular transfers, and daisy-chain flows.	M					
68	FR-CA-06	The solution shall support mule-account analytics, including turnover patterns, multiple small credits then cash-out, new/reactivated accounts with sudden high activity, shared identifiers (device, IP, phone, address) and network-level mule likelihood scoring.	M					
69	FR-CA-07	The solution shall support profiling and risk scoring of beneficiaries (e.g., age of relationship, number/diversity of originators, cross-bank flows) and highlight high-risk beneficiaries.	M					
70	FR-CA-08	The solution shall support analytics tailored to business/Corporate channels (e.g., maker-checker bypass attempts, bulk file anomalies, mass beneficiary uploads, off-hours approvals).	M					
71	FR-CA-09	The solution shall ingest and use telco-related risk signals (e.g., SIM swap, roaming status where available) to adjust risk for digital channels through Behavioral biometric solution deployed in the Bank	M					

72	FR-CA-10	The solution shall support channel-specific and segment-specific thresholds and rules, while reusing common features/models across channels where applicable.	M					
73	FR-CA-11	The solution shall support channel-wise dashboards and reports (e.g., fraud counts, detected amounts, alert volumes, false positives, hotspots by region/branch) with slicing by key attributes such as time, channel, product and customer segment.	M					
74	FR-CA-12	The solution shall allow simulation/back-testing of channel-specific rules/models on historical channel data before moving them to production.	M					
75	FR-CA-13	Analyze beneficiary profiles and identify risk clusters involved in mule rings, MLMs, scams, and fraudulent beneficiary hopping.	M					
76	FR-CA-14	The solution should support configuration and customization of OTMS rules for Branch transactions / staff accounts etc.	M					

7 Data Sandbox

Sr. No.	Requirement ID	Requirement Description	Mandatory (M) / Desirable (D)	Compliance (Yes/No) and Supporting Documents	Available as part of ALP (Yes / No)	Will be Provide as Customization (Yes / No)	Will be provided as Third Party ALP	Feasible (Yes/No)
77	FR-SB-01	The solution shall provide a secure, isolated sandbox environment for data scientists/analysts with separate compute and storage from production and role-based access.	M					
78	FR-SB-02	The sandbox shall support on-demand, template-based creation of new environments with time-bound access, without impacting production workloads.	M					
79	FR-SB-03	The sandbox shall support configurable replication/sub-sampling of production data (e.g., stratified samples) with automated refresh schedules and data freshness checks.	M					
80	FR-SB-04	All sandbox data containing customer/transaction information shall be anonymized/masked using approved techniques (e.g., tokenization, k-anonymity, l-diversity) as per Bank policy.	M					

81	FR-SB-05	The sandbox shall support Python, R and SQL with common data-science libraries (e.g., pandas, scikit-learn, TensorFlow/PyTorch, R tidyverse) and Spark where applicable.	M					
82	FR-SB-06	The sandbox shall provide notebook/IDE tools (e.g., Jupyter, RStudio, SQL editor) for interactive analysis and model development.	M					
83	FR-SB-07	The sandbox shall support experiment tracking (code version, data version, hyper-parameters, metrics) and model artifact versioning for reproducibility.	M					
84	FR-SB-08	The sandbox shall support model validation workflows (e.g., SHAP/LIME explainability, performance metrics, fairness checks) before promotion to staging/production.	M					
85	FR-SB-09	The sandbox shall support export/import of models and features into the production environment under Bank’s access control and approval processes.	M					
86	FR-SB-10	All sandbox access and actions (logins, queries, data read/write, model deployments) shall be logged in a tamper-evident audit trail.	M					
87	FR-SB-11	The sandbox shall use centralized secrets management (no hard-coded credentials) and ensure each project/team has isolated keys and data access.	M					

88	FR-SB-12	The bidder shall provide documentation, runbooks, and training for sandbox setup, safe data use, experiment tracking, and model promotion processes.	M					
89	FR-SB-13	The sandbox should support collaboration features (shared projects, comments, role-based sharing) while respecting access controls and auditability.	D					
90	FR-SB-14	The sandbox should support CI/CD integration for models (promotion path sandbox → staging → production with automated tests and peer review).	D					
91	FR-SB-15	Support advanced simulation capabilities such as Monte Carlo, agent-based, time-series simulation, stress testing, game-theory models, and "what-if" scenario analysis for fraud trends and detection models.	D					
92	FR-SB-16	Offer synthetic data generation tools to produce high-quality, statistically valid datasets for testing.	M					

8 Testing Environment & Rule Simulator

Sr. No.	Requirement ID	Requirement Description	Mandatory (M) / Desirable (D)	Compliance (Yes/No) and Supporting Documents	Available as part of ALP (Yes / No)	Will be Provide as Customization (Yes / No)	Will be provided as Third Party ALP	Feasible (Yes/No)
93	FR-RS-01	The solution shall provide a dedicated testing environment to test fraud rules and scenarios without impacting production.	M					
94	FR-RS-02	The testing environment shall maintain at least 3 months of rolling historical data (T+1 refreshed), including transactions, customer profiles and fraud outcomes.	M					
95	FR-RS-03	The solution shall provide a low-code/no-code rule simulator UI for drafting, editing and validating rules, with syntax/logic checks before execution.	M					
96	FR-RS-04	The rule simulator shall support back-testing rules on selected historical periods and datasets, with configurable filters (channel, product, segment, geography, etc.).	M					
97	FR-RS-05	The solution shall support simultaneous testing of multiple rules/scenarios in parallel, with	M					

		isolated resources per simulation to avoid interference.						
98	FR-RS-06	For each simulation run, the solution shall produce performance metrics including projected alert volumes, detection rate, and estimated false positive rate.	M					
99	FR-RS-07	The simulator shall support threshold and parameter sweeps (“what-if” analysis) for rules (e.g., amounts, counts, time windows) and compare results across runs.	M					
100	FR-RS-08	The solution shall support rule definition at transaction, account, customer, group/entity, and channel level, with clear precedence and hierarchy.	M					
101	FR-RS-09	The solution shall support creation and maintenance of inclusion and exclusion criteria (e.g., whitelists, exclusion, inclusion queues) within rules and scenarios.	M					
102	FR-RS-10	The solution shall maintain full version history of rules (who changed what, when), allow side-by-side comparison of versions, and enable rollback to prior versions.	M					
103	FR-RS-11	The solution shall implement maker-checker controls for rule	M					

		creation, modification and deployment, with configurable approval workflows.						
104	FR-RS-12	The solution shall support scheduled execution of test scenarios (e.g., daily/weekly) and manual on-demand runs.	M					
105	FR-RS-13	The solution shall provide a business rules engine capable of executing rules in real-time, near-real-time and batch modes, with performance monitoring.	M					
106	FR-RS-14	The simulator shall detect and flag duplicate or overlapping rules (logical similarity, parameter overlap) and suggest consolidation where appropriate.	M					
107	FR-RS-15	The solution shall allow assignment of weightages/priority to rules and support composite scoring using rule outputs where required.	M					
108	FR-RS-16	The solution shall support copying/cloning of existing rules to create new variants, with enforced editing and re-validation before activation.	M					
109	FR-RS-17	The solution shall provide visible evaluation results for rules (hit rates, success/ failure outcomes) and highlight rules with low utility for optimization or removal.	M					

110	FR-RS-18	The solution shall allow configuration of rule execution intervals and priority (e.g., high-risk rules executed first, or in-line vs. asynchronous), as per Bank policy.	M					
111	FR-RS-19	Generate detailed performance metrics from simulations including alert volumes, false positive rates, and detection rates with statistically significant results.	M					
112	FR-RS-20	Allow customizable alert scenarios supporting entity-specific, demographic, and behavioral segmentation with adaptive threshold management.	M					
113	FR-RS-21	Implement robust management of risk dimensions with multi-level access control, validation workflows, and impact assessment for threshold modifications.	M					
114	FR-RS-22	Maintain comprehensive audit trails for all rule changes capturing user identity, timestamps, reasons, and approval status with rollback capabilities.	M					
115	FR-RS-23	Enable creation of rules for non-monetary events such as address or phone modifications, PIN changes, device and IP updates, with fraud correlation.	M					

116	FR-RS-24	Support detailed rule version management with history, comparison, migration, merge conflict resolution, and lifecycle archiving and retention.	M					
117	FR-RS-25	Provide full logical and arithmetic operations support within rules including Boolean operators, conditional expressions, statistical functions, and date/time arithmetic.	M					
118	FR-RS-26	Support rule copying and templating for rapid creation of new rules with validation workflows.	M					

9 Enterprise Reporting & Dashboards

Sr. No.	Requirement ID	Requirement Description	Mandatory (M) / Desirable (D)	Compliance (Yes/No) and Supporting Documents	Available as part of ALP (Yes / No)	Will be Provide as Customization (Yes / No)	Will be provided as Third Party ALP	Feasible (Yes/No)
119	FR-RD-01	The solution shall provide self-service report and dashboard creation for business users via a low-code/no-code, drag-and-drop interface (no programming required).	M					
120	FR-RD-02	The solution shall provide standard visualization widgets (e.g., tables, KPI cards, bar/line charts, pie charts,	M					

		heat maps, bubble/cluster charts) for dashboards.						
121	FR-RD-03	The solution shall support interactive filtering, slicing and dicing by common fraud dimensions such as time, channel, product, geography, branch/region, and segment. Support diverse dashboard widgets (charts, heat maps, KPIs) with interactive design and flexible layout options.	M					
122	FR-RD-04	The solution shall support drill-down and drill-through from summary dashboards to detailed transaction / case / alert level views.	M					
123	FR-RD-05	The solution shall support scheduled and on-demand report generation and distribution (e.g., email, portal), with configurable frequency and recipient lists.	M					
124	FR-RD-06	The solution shall support export of reports and dashboard data in common formats including at least PDF, Excel, CSV and machine-readable formats (e.g., JSON/XML).	M					
125	FR-RD-07	The solution shall provide standard MIS reports for fraud operations (e.g., alerts by scenario, case volumes,	M					

		analyst productivity, false-positive rates, detection rates).						
126	FR-RD-08	The solution shall provide dashboards for management and executives showing key KPIs such as fraud loss prevented, fraud losses, alert volumes, case ageing and ROI.	M					
127	FR-RD-09	The solution shall provide network / linkage visualizations (e.g., entity graphs, money-flow diagrams) for identified fraud rings, SCAMS, MLM, mule networks and related entities.	M					
128	FR-RD-10	The solution shall provide case and investigator dashboards (e.g., open/in-progress/closed cases, turnaround time, backlog, investigator performance metrics).	M					
129	FR-RD-11	The solution shall provide channel-wise dashboards (cards, UPI, internet/mobile, ATM/POS, corporate) showing fraud and alert trends and key typologies per channel.	M					
130	FR-RD-12	The solution shall support regulatory and audit reporting requirements, using governed “gold” datasets, with ability to reproduce reports for historical periods.	M					

131	FR-RD-13	The solution shall support role-based access to reports/dashboards, controlling which users can view, create or modify specific content and underlying data.	M					
132	FR-RD-14	The solution shall support near-real-time or real-time refresh of key dashboards (e.g., alerts, high-risk channels) with configurable refresh intervals.	M					
133	FR-RD-15	The solution shall provide business-user interfaces (e.g., for department heads) with simplified, high-level overviews and limited technical detail.	M					
134	FR-RD-16	The solution shall store historical reports and dashboard snapshots in an auditable repository with search and retrieval for at least the period defined by Bank policy.	M					
135	FR-RD-17	Enable users to switch between no-code environments and advanced coding interfaces (SQL, Python) for complex queries.	D					
136	FR-RD-18	Enable drill-through from summaries to detailed underlying data with hierarchical navigation for root cause analysis.	M					

137	FR-RD-19	Integrate modules for data preparation, exploration, visualization, and administration with validation of data quality.	M					
138	FR-RD-20	Visualize account linkages, transaction flows, customer profiles, and network relationships to support fraud investigation.	M					
139	FR-RD-21	Allow business users to create custom dashboards and reports using intuitive graphical interfaces and drag-and-drop design.	M					
140	FR-RD-22	Provide real-time or near-real-time data refresh on dashboards and reports, configurable per user or report needs.	M					
141	FR-RD-23	Integrate workflows and MIS for Banking Ombudsman and internal complaint handling with end-to-end tracking and role-based access.	M					
142	FR-RD-24	Maintain secure online portals for Ombudsman complaint entry with mandatory fields and real-time progress tracking.	D					
143	FR-RD-25	Provide dashboards distinguishing analyst-handled vs. IVRS-handled calls with detailed volume reports.	M					
144	FR-RD-26	Provide cross-channel aggregate dashboards comparing risk profiles and fraud trends.	M					

145	FR-RD-27	Present financial impact analytics including fraud blocked amounts, savings, false positives, and cost-benefit analyses.	M					
146	FR-RD-28	Support trend analysis dashboards with advanced filtering across key dimensions including time, geography, and risk categories.	M					
147	FR-RD-29	Provide fraud typology dashboards highlighting emerging patterns and comparative seasonal trends.	M					
148	FR-RD-30	Deliver customer segment analysis dashboards showing fraud incidence across demographics and account types.	D					
149	FR-RD-31	Display prior fraud incidents, linked transactions, and expandable relationships within detailed case views.	M					
150	FR-RD-32	Provide performance dashboards tracking analyst productivity, accuracy, and development progress.	M					
151	FR-RD-33	Present system health dashboards showing ingestion latency, throughput, data quality, and availability.	D					
152	FR-RD-34	Deliver board-level dashboards consolidating risk metrics, governance oversight, and risk appetite monitoring.	M					

153	FR-RD-35	Provide role-specific user interfaces tailored for fraud analysts, investigators, business users, call analysts, and administrators.	M					
154	FR-RD-36	Enable simplified dashboards for business users with executive KPIs, strategic planning tools, and automated report generation.	M					

10 Case Management

Sr. No.	Requirement ID	Requirement Description	Mandatory (M) / Desirable (D)	Compliance (Yes/No) and Supporting Documents	Available as part of ALP (Yes / No)	Will be Provide as Customization (Yes / No)	Will be provided as Third Party ALP	Feasible (Yes/No)
156	FR-CM-01	The solution shall provide full case lifecycle management (creation from alerts or suo-motu, assignment, investigation, escalation, closure, archival). Provide comprehensive case management capabilities including automated case creation, assignment based on skills/workload, dynamic prioritization, lifecycle tracking, and archival per retention policies.	M					
157	FR-CM-02	The solution shall support configurable workflows and statuses for fraud cases, including SLA/aging tracking and escalation rules.	M					

158	FR-CM-03	The solution shall allow attaching and managing evidence (documents, screenshots, call recordings, notes) within each case, with basic tagging and search.	M					
159	FR-CM-04	The solution shall log all key case activities (view, edit, status change, assignment, closure, export) with user, timestamp and action in an immutable audit log.	M					
160	FR-CM-05	The solution shall support role-based views and permissions for cases (e.g., investigator, supervisor, admin) with control over who can view/modify/escalate.	M					
161	FR-CM-06	The solution shall support linking related cases and transactions (e.g., by common customer, account, device, IP, beneficiary) and display relationships clearly.	M					
162	FR-CM-07	The solution shall support search and filtering of cases by key attributes (e.g., ID, customer, account, channel, typology, status, priority, date range).	M					
163	FR-CM-08	The solution shall allow capture of case outcomes and dispositions (e.g., confirmed fraud, false positive, write-off, recovered) with standardized reason codes.	M					

164	FR-CM-09	The solution shall support basic collaboration on cases (e.g., comments, internal notes, task assignment) with visibility of who did what and when.	M						
165	FR-CM-10	The solution shall support integration with Bank CRM and PRM/alert systems etc. to share context (alerts, customer info, actions taken) and avoid duplicate data entry.	M						
166	FR-CM-11	The solution shall provide case dashboards (per investigator/team) showing workloads, ageing, SLA breaches, and performance metrics.	M						
167	FR-CM-12	The solution shall support user based regulatory documentation needs (e.g., export of full case file with timeline, evidence and audit trail) in standard formats (e.g., PDF)	M						
Investigator Workbench & Data Exploration									
168	FR-CM-13	The solution shall provide an investigator workbench showing consolidated context for each case (customer, accounts, transactions, alerts, external intelligence hits).	M						
169	FR-CM-14	The workbench shall support drill-down from a case to detailed transaction, device, channel and session information.	M						

170	FR-CM-15	The solution shall provide interactive network/link analysis views (graphs) showing relationships among customers, accounts, devices, IPs, beneficiaries and cases.	M					
171	FR-CM-16	The network view shall support expanding/collapsing nodes, filtering by attributes (e.g., channel, typology, time) and highlighting high-risk entities and links.	M					
172	FR-CM-17	The workbench shall display risk scores and key contributing factors/reason codes for transactions/entities under investigation.	M					
173	FR-CM-18	The solution shall support real-time or near-real-time data views for investigators (new alerts/transactions appearing without manual refresh, within set intervals).	M					
174	FR-CM-19	The solution shall support powerful search/filter across live and historical data (e.g., by customer, account, device, IP, amount, MCC, geography, typology).	M					
175	FR-CM-20	The solution shall support grouping of related alerts into network or multi-hop “cases” to show the full chain of activity to investigators.	M					

176	FR-CM-21	The solution shall allow investigators to flag entities (e.g., mule, scam, benign) and propagate this label to linked entities for future detection.	M					
177	FR-CM-22	The solution shall allow exporting investigation views (e.g., entity graphs, transaction lists) in standard formats (e.g., image/PDF/CSV) for external sharing.	M					
178	FR-CM-23	The solution shall provide investigator performance dashboards (per user/team) showing key metrics such as cases handled, TAT, hit rates, false-positive ratios.	M					
179	FR-CM-24	The solution shall support compliance with audit and regulatory requirements by maintaining detailed logs of investigator actions and data access in the workbench.	M					
180	FR-CM-25	Enable fraud analysts to initiate ad-hoc investigations triggered by alerts or data anomalies with flexible, customizable workflows and risk-based prioritization.	M					
181	FR-CM-26	Provide evidence management with secure digital attachment support, searchable metadata, chain-of-custody logging, and export capabilities for regulatory compliance.	D					

182	FR-CM-27	Maintain real-time case status management with role-based visibility, automated notifications on updates, status logging, and outcome documentation.	M					
183	FR-CM-28	Support collaboration features including shared commenting, file attachments with version control, messaging, task assignment, and team performance analytics.	M					
184	FR-CM-29	Integrate external data sources such as watchlists, regulatory databases, sanctions lists, and law enforcement information to enrich investigation context.	M					
185	FR-CM-30	Facilitate comprehensive case documentation, automated report generation, versioning, export in multiple formats, and secure distribution.	M					
186	FR-CM-31	Support case organization features including bookmarking, annotation, priority classification, peer review workflows, audit preparation, and knowledge sharing.	D					
187	FR-CM-32	Provide dynamic fraud network visualization with interactive nodes, multi-layer analysis, temporal relationships, clustering, and key player identification.	M					

188	FR-CM-33	Support dashboard personalization allowing investigators to customize widgets, layouts, KPIs, filters, and refresh rates with saved profiles.	D					
189	FR-CM-34	Facilitate detailed transaction drilling including location, device information, related entities, and contextual enrichment.	M					
190	FR-CM-35	Allow seamless switching between live and historical data views preserving user context and enabling comparative analysis.	D					
191	FR-CM-36	Provide immediate alert notifications through email, and SMS channels with customization and escalation workflows.	M					
192	FR-CM-37	Generate summary reports on investigator activity and fraud analyst effectiveness accessible to administrative users with scheduling.	M					
193	FR-CM-38	Support real-time collaboration tools including shared views, messaging, annotations, concurrent case editing, and team performance tracking.	D					

11 Data Management & Quality (Validation, Lineage, Governance)

Sr. No.	Requirement ID	Requirement Description	Mandatory (M) / Desirable (D)	Compliance (Yes/No) and Supporting Documents	Available as part of ALP (Yes / No)	Will be Provide as Customization (Yes / No)	Will be provided as Third Party ALP	Feasible (Yes/No)
194	FR-DM-01	The solution shall maintain a centralized logical data model for fraud analytics (customer, account, transaction, device, external intel). Model changes shall be version-controlled with documented impact.	M					
195	FR-DM-02	The solution shall support configurable data validation rules per source (schema, mandatory fields, type/length, ranges, formats, referential checks).	M					
196	FR-DM-03	The solution shall calculate and store data-quality metrics (e.g., completeness, null rates, error rates) and flag datasets breaching configurable thresholds.	M					
197	FR-DM-04	The solution shall maintain a data catalog with metadata for all fraud-relevant datasets/fields (description, source, update frequency, owner, sensitivity).	M					

198	FR-DM-05	The solution shall provide end-to-end lineage at least at table/field level, from source through transformations to marts/models/reports, viewable via UI/API.	M					
199	FR-DM-06	The solution shall support time-based versioning (“time travel”) for key fraud datasets, allowing queries “as of date/time” within Bank retention policy (e.g., 7 years).	M					
200	FR-DM-07	The solution shall support configurable retention and archival per data category (raw, curated, model outputs, logs) with automated tiering and purging as per policy.	M					
201	FR-DM-08	The solution shall maintain clearly identified curated (“gold”) datasets for fraud use, which are reconciled, de-duplicated and validated.	M					
202	FR-DM-09	The solution shall provide configurable de-duplication for key entities/transactions with logging of de-duplication decisions.	M					
203	FR-DM-10	The solution shall support entity resolution/linking across systems (e.g., Core, CRM, PRM, DWH, external lists) to create unified customer/account views.	M					

204	FR-DM-11	The solution shall enforce role-based access control at schema/table/column level and apply masking/redaction for sensitive attributes as per Bank policy.	M					
205	FR-DM-12	The solution shall auto-detect and classify PII-like fields (e.g., PAN, Aadhaar, phone, email) when new datasets are onboarded and default them to masked access.	M					
206	FR-DM-13	The solution shall support non-production environments using masked/anonymized or synthetic data, preventing exposure of live PII or sensitive financial data.	M					
207	FR-DM-14	The solution shall provide data-quality and lineage dashboards/reports (e.g., data-quality scores, validation errors, reconciliation status) for data owners/stewards.	M					
208	FR-DM-15	The solution shall maintain an immutable audit log of key data-management changes (schemas, rules, retention, masking, manual corrections) with user, time, before/after.	M					
209	FR-DM-16	The solution shall ensure data handling, retention, masking and access controls comply with Bank policies and applicable regulations (RBI, DPDP, GDPR where relevant).	M					

Advanced Analytical Layer Requirements									
210	FR-AL-01	large language models (LLMs) to be used within the solution (e.g., for analyst assistance), they shall run under Bank-approved data-governance controls and shall not send Bank data to unapproved external services.	D						
211	FR-AL-02	LLM-based components shall not perform automated adverse actions (e.g., blocking/unblocking accounts or channels) without explicit human approval and auditable workflows.	D						
212	FR-AL-03	LLM-based components shall support prompt and output controls (e.g., templates, content filters) and maintain logs of prompts and responses for audit and investigation	D						
213	FR-AL-04	The solution shall support using complaint and case outcome analytics to identify rule/model gaps and recommend changes (e.g., new typologies, threshold tuning, new features) for review by Bank analysts.	M						
214	FR-AL-05	The solution shall ingest and use existing risk scores produced by the Bank's Analytics platform (e.g., customer vulnerability scores, mule risk scores) as features or inputs into fraud scoring.	M						

215	FR-AL-06	The solution shall integrate with the Bank's existing Analytics Data Lake to ingest curated datasets and model outputs (e.g., customer vulnerability scores) for use in fraud analytics.	M						
216	FR-AL-07	The solution shall ingest complaint data from the Bank's CRM (including complaint type, channel, amounts, timestamps, resolutions) for analytics and correlation with fraud cases and alerts.	D						
217	FR-AL-08	The solution shall support analytics to identify patterns in complaints (e.g., recurring products/channels, disputed transaction types) and highlight potential rule/model gaps.	D						
218	FR-AL-09	The solution shall support complaint-to-fraud correlation (e.g., mapping complaints to underlying alerts/cases and typologies) and provide dashboards for complaint-driven fraud insights.	D						
219	FR-AL-10	The solution shall support workflows and MIS for Banking Ombudsman/Internal Ombudsman complaints and advisories, including routing, tracking, status and turnaround time.	D						

220	FR-AL-11	The solution shall provide an online portal/dashboard for Ombudsman offices and circles to submit, track and analyze complaints/advisories related to digital/fraud transactions.	D					
221	FR-AL-12	The solution shall support generation of standard complaint and Ombudsman reports (volumes, ageing, status, outcomes, escalation patterns) as per Bank/regulatory requirements.	D					
222	FR-AL-13	The solution shall maintain behavioural baselines per customer and per device using at least a configurable minimum of 90 days of historical activity (where available).	D					
223	FR-AL-14	The solution shall profile key behavioural dimensions, including login patterns, time-of-day usage, transaction frequency/amount patterns and payee/beneficiary behaviour.	D					
224	FR-AL-15	The solution shall integrate and consume behavioural biometric signals (e.g., device/behavioural provider outputs) where available, as features in risk scoring.	D					
225	FR-AL-16	The solution shall compute and maintain device-level trust scores (e.g., 0–100) and show device–account networks (shared devices, device farms, orphan devices).	D					

226	FR-AL-17	The solution shall maintain geolocation baselines (home/work/travel clusters) and detect anomalies including new/distant locations and impossible travel patterns.	D					
227	FR-AL-18	The solution shall compute a unified Behavioural Risk Score (BRS) per event/entity by combining behavioural, device and geolocation indicators.	D					
228	FR-AL-19	The solution shall expose the BRS via APIs or message interfaces for use by fraud, AML and authentication systems in real-time or near-real-time.	D					
229	FR-AL-20	The solution shall support configuration of BRS-based thresholds and actions (e.g., step-up authentication, manual review) per channel, product and customer segment.	D					
230	FR-AL-21	The solution shall enable advanced ML Ops automation including automated data drift detection, continuous integration of new data, and model deployment rollback.	D					

Appendix E 2: Technical Specification & Non – functional Requirements

Sr. No.	Requirement ID	Requirement Description	Mandatory (M) / Desirable (D)*	Compliance (Yes/No) and Supporting Documents	Available as part of ALP (Yes / No)	Will be Provide as Customization (Yes / No)	Will be provided as Third Party ALP	Feasible (Yes/ No)
Performance & Scalability								
1	TR-PS-01	The solution shall support a sustained peak throughput of at least 22,000 transactions per second for high-risk real-time channels (e.g., UPI, cards, mobile/internet, EPAY, YONO).	M					
2	TR-PS-02	The solution shall meet end-to-end latency targets (from data receipt to fraud scoring/decision) as defined by the Bank for real-time and near-real-time channels.	M					
3	TR-PS-03	The solution shall support horizontal scaling (scale-out) of ingestion, processing, and storage layers without material performance degradation as transaction volumes grow.	M					
4	TR-PS-04	The data reservoir/lake and analytical marts shall support petabyte-scale storage and high-volume queries using partitioning, indexing and columnar storage for performance.	M					

5	TR-PS-05	The solution shall support multiple ingestion modes (real-time streaming, micro-batch, scheduled batch) and process data with sub-second latency for streaming and within defined SLAs for batch.	M					
6	TR-PS-06	The solution shall provide monitoring dashboards for performance (throughput, latencies, resource usage, error rates) and allow tuning based on these metrics.	M					
7	TR-PS-07	Analytical marts shall support fast multidimensional analysis (slice-and-dice, drill-down) using OLAP-style capabilities and pre-aggregated KPIs where required.	M					
8	TR-PS-08	The solution shall support optimized data organization (e.g., time-based and categorical partitioning, clustering) to reduce query scan times on large datasets.	M					
9	TR-PS-09	The solution shall support parallel processing of rules/models in real-time and batch modes with appropriate resource isolation and prioritization for high-risk channels.	M					
10	TR-PS-10	The solution shall support load balancing across nodes/components to handle concurrent users and workloads (ingestion, scoring, reporting, investigation) efficiently.	M					
Availability, RPO/RTO, DR								

11	TR-AV-01	The solution shall comply with the Bank’s IT and BCP/DR policies and support high availability for all critical components of the fraud analytics platform.	M					
12	TR-AV-02	The solution shall achieve a Recovery Point Objective (RPO) of near-zero and a Recovery Time Objective (RTO) of ≤ 15 minutes for critical services, as per Bank policy.	M					
13	TR-AV-03	The solution shall provide automatic failover for critical services (ingestion, scoring, data stores) to standby nodes/sites without data loss or manual intervention.	M					
14	TR-AV-04	The solution shall support regular backups and point-in-time restore for core data stores (reservoir, lake, marts, configuration, models) in line with Bank backup and retention policies.	M					
15	TR-AV-05	The solution shall support DR drills and provide procedures/scripts to validate recovery of data and services within defined RPO/RTO targets.	M					
16	TR-AV-06	The solution shall monitor health and availability of data feeds and internal components and generate alerts for failures, delays or degradation in ingestion and processing pipelines.	M					

17	TR-AV-07	Historical data snapshots and time-travel capabilities shall be preserved across backup/restore and DR processes to support investigations and regulatory reviews.	M						
18	TR-AV-08	The solution shall support configurable data retention and archival policies, including automated aging and movement to archive tiers without impacting availability of current data.	M						
Security and compliance (Refer Appendix 'T' – compliance is mandatory)									
19	TR-SC-01	The solution shall comply with the Bank's Information Security Policy, IT Policy, Data Governance Policy, and relevant RBI Master Directions and circulars.	M						
20	TR-SC-02	All data in transit shall be protected using **TLS 1.2 or higher**; all sensitive data at rest shall be protected using **AES-256** or database-native Transparent Data Encryption (TDE), as applicable.	M						
21	TR-SC-03	The solution shall enforce **role-based access control** (RBAC) and principle of least privilege across UI, APIs and data stores, including field-level masking/redaction where required.	M						
22	TR-SC-04	The solution shall support integration with the Bank's identity and security infrastructure (e.g., AD/LDAP, SSO, MFA, IDAM, SIEM, DAM, AV, DLP, ERM) as per Bank standards.	M						

23	TR-SC-05	The solution shall support **maker-checker** (dual-control) for critical changes (rules, models, configurations, access rights) with approval workflows and audit trail.	M					
24	TR-SC-06	The solution shall maintain comprehensive, tamper-evident audit logs of key user and system activities (logins, configuration changes, data access, model deployments, rule modifications).	M					
25	TR-SC-07	The solution shall implement PII and sensitive data protection including automated detection/classification, masking/tokenization, and restricted access to unmasked data with full logging.	M					
26	TR-SC-08	The solution shall support separation of production and non-production environments and prevent unapproved export of live PII/sensitive data into non-production.	M					
27	TR-SC-09	The solution shall support secure test data management (masking/anonymization, synthetic data generation, PII scanning) to ensure non-production environments are non-sensitive.	M					
28	TR-SC-10	The solution shall comply with applicable privacy regulations (e.g., DPDP Act, GDPR where relevant) and support evidence production (logs, configurations) for audits.	M					

29	TR-SC-11	Any external data sharing or exports (e.g., to regulators or partners) shall be controlled via approval workflows, redaction/masking policies and secure transmission mechanisms.	M					
30	TR-SC-12	The solution shall restrict internet and general network access from data processing environments; only approved connectors/integration endpoints shall be allowed, as per Bank’s SDLC and security processes.	M					
31	TR-SC-13	The solution shall provide dashboards/reports for security and compliance monitoring (e.g., data quality and lineage, security events, access violations, ingestion anomalies).	M					
Extensibility & Maintainability								
32	TR-EM-01	The solution shall support configuration-driven onboarding of new data sources, channels, products and external feeds without changes to core product code.	M					
33	TR-EM-02	The solution shall provide a governed mechanism to extend data models, features, rules and models (e.g., adding fields, new rules, new model endpoints) with versioning and impact analysis.	M					

34	TR-EM-03	The solution shall support CI/CD pipelines for application, configuration and model deployments, aligned with the Bank's SDLC, including automated testing and rollback.	M					
35	TR-EM-04	The solution shall provide APIs and standard connectors for integration with existing and future Bank systems (core, CRM, PRM, data warehouse, data lake, sandboxes, BI tools).	M					
36	TR-EM-05	The solution shall maintain a clear separation of concerns between ingestion, storage, analytics, rules, models and presentation layers to ease maintenance and future enhancements.	M					
37	TR-EM-06	The solution shall support environment consistency (dev, test, staging, production) via infrastructure-as-code/ configuration-as-code and controlled promotion processes.	M					
38	TR-EM-07	The solution shall provide comprehensive technical documentation, runbooks, and training for administrators, developers and operations teams.	M					
39	TR-EM-08	The solution shall allow the Bank's analytics team to deploy and manage their own AI/ML models (Python/R, PMML/ONNX, APIs) within the platform, reusing the same monitoring and governance.	M					

40	TR-EM-09	The solution shall support feature and model reuse across channels and products (e.g., a feature developed for UPI can be reused for cards with channel-specific thresholds).	M					
41	TR-EM-10	The solution shall support configurable retention of configurations (rules, mappings, models) and maintain historical versions for troubleshooting and rollback.	M					
42	TR-EM-11	The solution shall support modular upgrades and patches (component-level where feasible) without requiring full system downtime beyond agreed maintenance windows.	M					
43	TR-EM-12	The solution shall be designed so that new analytical use cases (e.g., additional channels, new complaint types, new external feeds, new models) can be onboarded through configuration and governed extension processes without core re-engineering.	D					
44	TR-EM-13	Implement zero-trust security for pipeline access with RBAC, MFA, privileged access management, and audit trails.	M					
45	TR-EM-14	Intelligent tiered storage with Gold (curated), Silver (validated), Bronze (raw), and Archive zones with lifecycle management.	M					

46	TR-EM-15	Store curated data warehouse optimized for fraud analytics with ETL/ELT pipelines for enrichment and validation.	M					
47	TR-EM-16	Analytical marts with fraud-specific dimensional models supporting risk evaluation, transaction analysis, and regulatory reporting.	M					
48	TR-EM-17	Support ingestion of additional emerging data ingestion protocols and formats beyond mandatory standards with seamless integration.	D					
49	TR-EM-18	Provide enhanced data anonymization and synthetic data generation for development, testing, and privacy-preserving analytics.	M					
50	TR-EM-18	The AP should adhere to AI/ML Model Governance policy of the Bank i.e. Enterprise Model Risk Management Policy and AI Based Emerging Technologies Policy.	M					
51	TR-EM-19	The AP should provide or integrate Application / system / performance monitoring tools alongwith the pre-scheduled reports for Application performance Monitoring	M					

*Note

1. **Mandatory (M)**: Requirements marked as *Mandatory* are critical for the intended functioning, security, compliance, and minimum scope of the Analytical Layer Platform. They:
   a. Must be designed, developed, configured, integrated, tested and accepted before Go-Live of the ALP; and

b. Are a pre-requisite for Go-Live sign-off under this RFP.

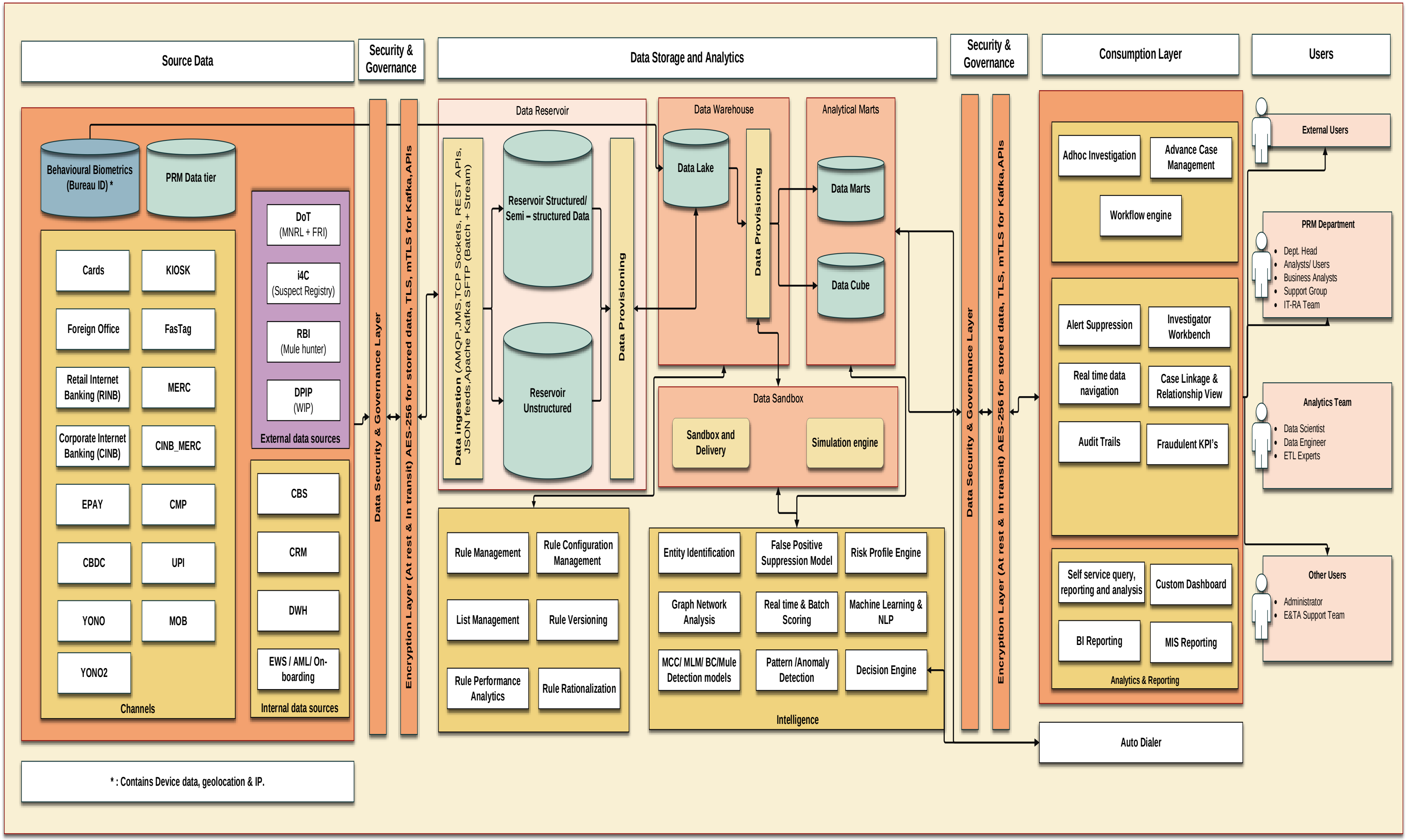
2. **Desirable (D)**: Requirements marked as *Desirable* are important for enhancing coverage, efficiency, analytics depth, or future-readiness of the ALP. They:

   a. Are not a pre-condition for initial Go-Live, but

   b. Must be delivered within the overall contract period, as part of the implementation roadmap and/or subsequent releases, in consultation with the Bank; and

   c. Will be planned, prioritized and implemented through the agreed change / release management process during the contract term.

Appendix E 3: Indicative Solution Architecture:



Appendix E 4: Capacity Building

Application Provider should be required to provide training to the users associated with the usage of Analytical Layer / Platform (ALP), to enable them to effectively operate and perform the relevant functions. AP shall carry out comprehensive training needs analysis and design the training program accordingly.

I. AP shall provide one week of customized training (depending on proposed role) and two refresher courses every year to PRM Department

II. AP shall involve the trainers of OEMs in conducting training of specialized COTS products/modules, if proposed. The Application Provider shall provision for training man-days on specialized tools and technologies used for the project.

III. The schedule and content of the training will be finalized in consultation with the Bank.

IV. AP shall prepare a detailed training plan, including the mode of training, training needs at various levels, the proposed curriculum, duration of each training program and the entry and exit criteria.

V. The schedule and content of the training of trainers will be finalized in consultation with the Bank.

VI. AP shall prepare a trainer tool kit and training material to assist the trainers in conducting training. AP shall ensure that the training content is relevant to the role of the end users. AP shall incorporate and implement changes suggested by the trainers.

VII. AP shall create necessary performance support material such as user manual, job aids, online reference manual, frequently asked questions, training documentation etc.

VIII. AP shall design and implement a system for capturing feedback on training.

IX. AP shall design and develop a training environment with training data to enable Bank users at all levels to have hands on training on some of the key modules like case viewer.

X. Training of Bank personnel to be conducted by the AP are detailed in Table below:

S. No.	User Group	Description	Number of people to be trained	Training Module	Frequency /year

			annually		
a)	Core user	Personnel(s) deployed in PRM Division And /or IT (RA) Team and/or Analytics team	25	Analytical tools e.g. ALP, Excel, SQL, creation of algorithms, scripts, connectors, data modelling, programming language, Big Data Analytics, Data Science, Advance Analytics, ETL techniques, parametrization, error handling, deployment of various products/ packages training on reports, Security, and Administrator training etc. procured/developed for The Bank	Twice
b)	Administrator user	PRM officers	10	Training on the latest technologies in the Data Analytics, statistical tools and related technologies	Twice

XI. The AP must ensure that the training sessions held are effective and that the attendees would be able to undertake their work efficiently. For this purpose, it is necessary that the effectiveness of training sessions is measured. AP will prepare a comprehensive online feedback form that will capture necessary parameters on measuring effectiveness of the training sessions.

XII. For each training session, the AP will categories the feedback on a scale of 1 to 5, where 5 will denote excellently and 1 will denote unsatisfactory.

XIII. The training session would be considered effective only after the cumulative score of the feedback [sum of all feedback divided by number of attendees] is more than 3 out of 5.

Appendix E 5: Manpower Requirement

For a project of such a large scale and complexity, it is imperative that the AP must deploy best of class professionals to ensure successful execution of the project. The AP will in its proposal include the names and detailed curriculum vitae of their key personnel who will be working full time on the project.

Post Go-Live, Bank will require manpower resources for the on-going development. the Indicative Resource requirements post Go-live is as follows:

Role	Year 1	Year 2	Year 3	Year 4	Year 5
	No. of*resources	No. of resources	No. of resources	No. of resources	No. of resources
PM + Delivery Leads	1	1	1	1	1
Solution Architect	1	1	1	1	1
Data Scientist	2	2	2	2	2
Data Engineers	2	2	2	2	2
Application / Integration Developer	1	1	1	1	1
MLOps / DevOps Engineers	1	1	1	1	1
Infrastructure Architect / Engineer	1	1	1	1	1
Business Analyst – Fraud / Risk	1	1	1	1	1
ETL/ELT Engineers	1	1	1	1	1
Knowledge management	1	1	1	1	1
BI Developers	1	1	1	1	1
QA + Automation	1	1	1	1	1
SMEs (Fraud + Risk Domain)	1	1	1	1	1
Total Manpower	**15**	**15**	**15**	**15**	**15**

Similarly, Post Go-live On-site technical support requirement by 24*7 is as below:

ONSITE TECHNICAL SUPPORT SERVICES		
Sr. No.	Item	No of Resources*
1.	OTS Charges for L3 Resource	10
2	OTS Charges for L2 Resource	6
3	OTS Charges for L1 Resource	1
	Total	17

*This is only indicative the Bank reserves the right to increase or decrease the number of resources, with prior intimation to the AP.

1) AP has to propose named resources for all the key roles as mentioned in the technical evaluation criteria of this RFP. The proposed resources must be part of the project team and must be available for discussion with the client at client location.
2) AP shall provide the required resources to design and implement the solution including number, skill sets and duration and provision the same for implementation of this project.
3) AP has to necessarily maintain a team of requisite size of skilled professionals as per the requirements of the project.
4) AP shall propose the team structure and deployment plan of key resources onsite and offsite for the project. The resources proposed must not be changed unless replaced with equivalent or higher qualification and experience with prior concurrence of the Bank.
5) AP must have project managers and other personnel required to be provisioned full time to be stationed at client location for the duration of the project, and the same should be reflected in the proposed team structure and deployment structure.
6) AP shall ensure requisite support from the OEM for various aspects of project including configuration, customization, sizing, performance tuning and implementation support.
7) The resources detailed is the minimum requirement and AP is at liberty to field additional resources for achieving objectives of the project. The list below gives number of minimum resources that AP shall deploy onsite (full time) at The Bank premise which may change depending on the project requirements.
8) AP shall assess the requirement of resources for managing the operations of ALP solution including number, skill sets and duration and provision the same for operations management of this project.
9) AP shall deploy suitable technical resources for ALP as per activities expected to be carried out, and all the resources should be trained in the use of the deployed tools, technologies and should have requisite functional knowledge.

10) AP shall ensure that all the resources deployed at The Bank undergo suitable trainings in relation to security aspects of the project and maintain the confidentiality of data.
11) During the course of the contract, if it becomes necessary to replace any of the key personnel, AP shall forthwith with due consent from The Bank provide as a replacement a person of equivalent or better qualifications and experience than the resource being replaced.
12) The resources deployed for the project may be appropriately distributed in teams as per the requirements of the workload.
13) The manpower shall be deployed by the AP for executing operations, management and maintenance of the ALP solution, as per terms specified in this RFP and agreed with The Bank
14) AP is required to deploy the team, subsequent to go-live of Fraud Analytics solution which is defined as Milestones.
15) AP resources will have to work in collaboration with the Bank Officers and collectively work iteratively through the information available to structure the data for achieving the desired outcome
16) The number of resources committed for the proposed duration must be maintained by AP at all times.

Key Resources of the AP
The Project Team shall at a minimum include expertise and experience in the following disciplines:

Note: The Bank reserves the right to interview proposed candidates prior to onboarding and to reject any candidate deemed unsuitable, and may require the AP to replace any resource whose performance does not meet the Bank's requirements.

Table: Illustrative ALP resource qualifications

Profile Title	Qualification	Total Experience	Relevant / Prior Experience (Indicative)
PM + Delivery Leads	Bachelor's in Engineering/IT/CS or equivalent; MBA/PMP/Prince2 preferred	12+ years	8+ years managing large IT programs; 5+ years in banking/financial services; prior delivery of analytics or fraud/risk management platforms.
Solution Architect	Bachelor's in Engineering/IT/CS or equivalent; TOGAF/architecture certification preferred	10+ years	5+ years as solution architect for large-scale, high-availability systems; experience in data/analytics platforms and integration-heavy solutions.
Data Scientist	Master's in Statistics/Mathematics/CS/Data Science or equivalent	5+ years	3+ years in ML for financial services; hands-on with fraud/risk analytics, anomaly detection, graph/NLP preferred; strong Python/ML stack skills.
Data Engineers	Bachelor's in Engineering/IT/CS or equivalent	5+ years	3+ years building data pipelines (batch + streaming) on big data or modern data platforms; exposure to financial/banking data preferred.
Application / Integration Developer	Bachelor's in Engineering/IT/CS or equivalent	5+ years	3+ years in backend/frontend or integration development (APIs, ESB, MQ, microservices); experience integrating with banking/enterprise systems.

MLOps / DevOps Engineers	Bachelor’s in engineering/IT/CS or equivalent; DevOps/Cloud certifications preferred	5+ years	3+ years in CI/CD, containerization, orchestration; experience deploying and monitoring ML models and/or analytics workloads in production.
Infrastructure Architect / Engineer	Bachelor’s in engineering/IT/CS or equivalent; infra/cloud certifications preferred	8+ years (Architect) / 5+ (Eng.)	4+ years designing/implementing infra for mission-critical systems; experience with HA/DR, performance tuning, and secure banking environments.
Business Analyst – Fraud / Risk	Bachelor’s in commerce/finance/IT; MBA/FRM/related certification preferred	7+ years	4+ years in banking fraud/risk operations or solutions; experience in requirement gathering for fraud systems and regulatory reporting.
ETL/ELT Engineers	Bachelor’s in engineering/IT/CS or equivalent	5+ years	3+ years in ETL/ELT development on DWH/lake; experience with CDC, data validation, and performance optimization; BFSI exposure preferred.
Knowledge Management	Bachelor’s degree in any discipline; specialization in documentation/training preferred	5+ years	3+ years in IT project documentation and knowledge management; experience creating user manuals, SOPs, and training materials for enterprise systems.
BI Developers	Bachelor’s in engineering/IT/CS or equivalent	5+ years	3+ years developing dashboards, reports, and analytics in BI tools; experience with banking/fraud KPIs and drill-down analytics preferred.
QA + Automation	Bachelor’s in engineering/IT/CS or equivalent; testing certifications preferred	5+ years	3+ years in functional and automation testing; prior testing of data/analytics or fraud/risk platforms; experience with performance testing desirable.

SMEs (Fraud + Risk Domain)	Bachelor’s in commerce/finance/Banking; advanced certifications (e.g., CFE, FRM) preferred	10+ years	7+ years in bank fraud risk management, investigations, or fraud operations; hands-on experience with enterprise fraud management systems.

Price Bid

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

Name of the Bidder:

COMMERCIAL TABLE: SUMMARY OF COST					
Sr. No.	Item	Reference Table	Total Cost in Rs.	Total Amount in Rupees	Proportion to Total Cost (in percentage)
1.	Analytical Layer Licenses Including One year warranty and 5 Years ATS cost	A			
2	ALP Solution Installation, Implementation, Configuration, and Integration Cost	B			
3	Onsite Technical Support (OTS/FMS) Cost	C			
4	Resource Cost for on-going development	D			
Total Cost of Operations (TCO)*		A+B+C+D			

TABLE A

Analytical Layer Platform / Solution License Cost							
Sr. No.	Item	Year 1	Year 2	Year 3	Year 4	Year 5	Total Cost
1.	Enterprise License Fee for ALP to be provided with high availability in both DC & DR as per the specifications in the RFP						
2	Annual Technical Support Cost for five years maintenance of ALP required for successful implementation of the solution as per the technical specifications/ requirements/ scope of work as described in the RFP.						
Total Cost of Table 'A'							

TABLE B

<table>
<tr><th colspan="4">INSTALLATION, IMPLEMENTATION, CONFIGURATION AND INTEGRATION OF ALP SOLUTION</th></tr>
<tr><th>Sr. No.</th><th>Item</th><th>Description</th><th>Total Cost</th></tr>
<tr><td>1.</td><td>Phase – 1: Integration with Channels, CBS, Datawarehouse, PRM Application & Dialer and Ingest data from these sources</td><td>
<table>
<tr><th>Channels</th><th>Internal Sources</th></tr>
<tr><td>CARD</td><td>Core Banking (CBS)</td></tr>
<tr><td>CBDC</td><td>Datawarehouse</td></tr>
<tr><td>CINB_MERC</td><td>Existing PRM Application</td></tr>
<tr><td>CINB</td><td>Dialer</td></tr>
<tr><td>CMP</td><td></td></tr>
<tr><td>EPAY</td><td></td></tr>
<tr><td>FASTAG</td><td></td></tr>
<tr><td>FO</td><td></td></tr>
<tr><td>KIOSK</td><td></td></tr>
<tr><td>MERC</td><td></td></tr>
<tr><td>MOB</td><td></td></tr>
<tr><td>RINB</td><td></td></tr>
<tr><td>UPI</td><td></td></tr>
<tr><td>YONO</td><td></td></tr>
<tr><td>YONO2</td><td></td></tr>
</table>
</td><td></td></tr>
<tr><td>2</td><td>Development & Deployment of Core Analytics:</td><td>Core Analytics Application
• Case Management
• Rule Management
• Reporting & Dashboard
• Rule Simulator & Test Environment
• User Access Management
• Alert Management</td><td></td></tr>
<tr><td>3</td><td>Phase – 2 Peripheral and external sources integration</td><td>Integration with
• Behavior biometric solution
• CRM
• AML
• On-boarding channels
• DoT MNRL
• DoT FRI
• i4C suspect registry
• RBI Mule hunter
• RBI CFR repository
• DPIP
• NCRP portal</td><td></td></tr>
<tr><td>4</td><td>Development & Deployment of Advanced Analytics:</td><td>Development & Customization of Advanced Analytics
• AI-Based transaction scoring model
• Scam detection
• Mule Detection</td><td></td></tr>
</table>

		- Anomaly detection - False positive reduction - Network / Link & Graph analysis	
5	Development & Deployment of Peripheral Requirements	Peripheral Requirements - Offline Transaction Monitoring (OTMS) - AI Model for voice call analysis of analyst - Design specific workflows for operations, OTMS and Admin - integration of proposed ALP with the Bank's current security	
6	Documentation & Training	User training, SOPs, User-guides, and complete Documentation as mentioned in the RFP	
7	Additional Internal Integrations	Cost of 1 unit of additional internal Channel/Application to be Integrated with ALP (as and when required by the Bank) during the contract period	
8	Additional External Integrations	Cost of 1 unit of additional external Channel/Application to be Integrated with ALP (as and when required by the Bank) during the contract period	
9	Additional AI/ML Model Development & Deployment	Cost of 1 unit of additional AI/ML model to be developed & deployed within ALP (as and when required by the Bank) during the contract period	
		Total Cost of Table 'B'	

TABLE C

ONSITE TECHNICAL SUPPORT SERVICES								
Sr. No.	Item	No of Resources	Year 1	Year 2	Year 3	Year 4	Year 5	Total Cost
		Q*	total cost of resources per Annum					
1.	OTS Charges for L3 Resource	10						
2	OTS Charges for L2 Resource	6						
3	OTS Charges for L1 Resource	1						
Total Cost of Table 'C'								

***** Bank reserves the right to engage additional resources at the same cost during the contract period. Additional no L1 & L2/L3 OTS resources as and when required by the Bank should be provided by the bidder at the same rate as Table C.***

TABLE D

Manpower Requirements								
Sr. No.	Item	No of Resources	Year 1	Year 2	Year 3	Year 4	Year 5	Total Cost
		Q*	Unit cost per resource per Annum					
1	PM + Delivery Leads	1						
2	Solution Architect	1						
3	Data Scientist	1						
4	Data Engineers	1						
5	Application / Integration Developer	1						
6	MLOps / DevOps Engineers	1						
7	Infrastructure Architect / Engineer	1						
8	Business Analyst – Fraud / Risk	1						
9	ETL/ELT Engineers	1						
10	Knowledge management	1						
11	BI Developers	1						
12	QA + Automation	1						
13	SMEs (Fraud + Risk Domain)	1						
Total Cost of Table 'D'								

***** Bank reserves the right to engage additional resources at the same cost during the contract period. Additional no resources as and when required by the Bank should be provided by the bidder at the same rate as Table D. Total cost under table 'D' shall not be more than 25% of the Total cost of Operations (TCO)***

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				

<u>Name & Signature of authorized signatory</u>

<u>Seal of Company</u>

Appendix -G : Local Content

Certificate of Local Content

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

Date:

To,
____
____
____

Dear Sir,

Ref.: RFP No. : SBI:RMD/PRMD/2025-26/01 dated **02.01.2026**

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 **OEM**

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

Appendix -H : Bank Guarantee

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 ALP/ Service) (hereinafter referred to as **"Services")** to SBI in accordance with the Request for Proposal (RFP) No. **SBI:RMD/PRMD/2025-26/01** dated **02.01.2026**.

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-

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

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

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

iv. 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

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

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

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

Notwithstanding anything contained herein above:

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

ii. This Bank Guarantee shall be valid upto________________

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

Yours faithfully,

For and on behalf of bank.

____

Authorised official

Appendix -I : Bank Certificate

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

Date:

M/s.______________

____

Sub: Certificate of delivery, installation and commissioning

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

    a) PO No.__________________ dated ________________________ ___

    b) Description of the ALP __________________________________

    c) Quantity ____ _ _____

    d) Date of installation____

    e) Date of acceptance test _______________________________________

    f) Date of commissioning _______________________________________

2. Details of specifications of Software ALP 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 ALP.

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 ALP/Services is given under Para No. 2 above.

Signature ________________________

Name ________________________

Designation with stamp ___________________
____

Appendix-J : Penalties

Penalties

Service level category	SLA Measure	Penalty Calculation
During Implementation & pre-Go-Live		
Implementation timelines per stage	Achieve all agreed milestones and final go-live by due dates in approved Project Plan for each Stage	.1% of Total Cost per week of delay or part thereof; capped at 20% of Total Cost of operations (TCO)
Post Go-Live		
Application Availability (quarterly)	Minimum 99.90% uptime per quarter, 24x7x365, excluding approved planned maintenance	a) Uptime ≥ 99.90%: No penalty b) 99.90% > Uptime ≥ 99.50%: 1% of Annual ATS c) 99.50% > Uptime ≥ 98.50%: 2% of Annual ATS d) Uptime < 98.50%: 2% of Annual ATS + 1% of Annual ATS for every 0.10% drop (or part) below 98.50%.
Real-time transaction response time	ALP to respond to online authorization / validation requests from integrated channels within 50 milliseconds under normal operations or as agreed with the Bank	For each calendar day: a) If <= 1% of transaction / hour with response time >50 ms or as agreed with the Bank = 0.0025% of Annual ATS for each such instance in a day b) If > 1% of transaction / hour with response time >50 ms or as agreed with the Bank = 0.005% of Annual ATS for each such instance in a day E-g: If in 24 hours there are 5 hourly instances where response time for 1% of transactions are more than 50 ms than the penalty will be levied as below = 5* (0.005% of Annual ATS)

		Note: No penalty if delay is solely due to Bank-side infra / external network and vendor has properly raised/recorded the exception
Onsite resource availability	Maintain agreed onsite staffing (e.g. L1/L2, Data scientist, etc.) at Bank premises as per approved staffing plan and schedule	For absence or non-deployment of any key onsite resource, deduction of the pro-rata per-day cost of that resource from payments. AND 0.5% of total manpower Cost per day of absence, Capped at 20% Total Cost of operations (TCO) Note If replacement requested by Bank is not provided within 30 days, each subsequent day is treated as absence and penalised as above.
Security, vulnerability, Audit and compliance Gaps	Closure of Gaps identified based on Severity Levels: a) Critical > 8 hours from the time of incident reporting b) High > 48 hours from the time of incident reporting c) Medium >7 days from the time of incident reporting d) Low >1 Month from the time of incident reporting	0.5% of total Cost , Capped at 20% total Costof operations (TCO)

Note*

1. For the purpose of Penalty clause:
   i. Manpower cost is the cost provided by the Bidder under Table 'C' and Table 'D' of **Appendix F**
   ii. Implementation cost is the cost provided by the Bidder under Table 'A' and Table 'B' of **Appendix F**

2. Total of all penalties under the contract (Aggregate penalties) shall not exceed 20% of Total Cost of Operations (TCO). Crossing 20% of TCO is itself a material default. Bank may terminate, cancel PO and/or invoke PBG.
3. The uptime percentage would be calculated on quarterly basis and the calculated penalty amount would be adjusted from every subsequent ATS payment.
4. Penalties shall not apply to the extent a Service Failure is solely and directly attributable to:
   i. a duly notified Force Majeure event
   ii. failure/malfunction of Bank-side hardware/software/network or third-party provider engaged directly by the Bank, provided that the AP has promptly escalated and demonstrated reasonable mitigation efforts.
   iii. The burden of proof for such exclusions lie with the vendor.

Appendix-K : SLA

Service Level Agreement

SOFTWARE/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:

[1] Name & Complete Address of the Dept.

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

1.1 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

[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.

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 ……………. (name of the Software/ maintenance services) <*Strike off whichever is Inapplicable*>,[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

[6] Name of Software

manuals, design documents, process documents, data flow documents, data register, technical manuals, functional specification, software requirement specification, on-line tutorials/CBTs, system configuration documents, Data Dictionary, system/database administrative documents, debugging/diagnostics documents, test procedures, Review Records/ Test Bug Reports/ Root Cause Analysis Report, list of all Product components, list of all dependent/external modules and list of all documents relating to traceability of the Product as and when applicable etc.

1.1.7 "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 "Total 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. **SBI:RMD/PRMD/2025-26/01** dated **02.01.2026** 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 <*Strike off whichever is Inapplicable*> 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 **“COTS”** - Commercial off-the-shelf product(s). Any product quoted shall be treated as Commercially available Off-The-Shelf (COTS) product if it meets the below requirements:

1.1.17.1 It is readily deployable with or without customization to suit the specific process requirements and does not involve developing the application from scratch or major significant developments in the product; and

1.1.17.2 It has been implemented by at least 8 organizations; and

1.1.17.3 It is implemented and maintained by at least 3 implementation partners other than the OEM of the COTS Software and each partner should have done at least one implementation. At least one of the implementation partners should have presence in INDIA.

1.1.18 **“Prototype”**: A prototype is an early sample, model, or release of a product built to test a concept or process. A prototype is generally used to evaluate a new design to enhance precision by business analysts and users. In this project, it will be expected that the AP will showcase a concept which will have the screens of the respective use cases and user shall be able to navigate from one screen to other to understand the business process flow.

1.1.19 “**Days**”: All Working and Non-working days (365 days in a calendar year)

1.1.20 “**Non-Working Days**”: 2nd and 4th Saturday of every month, Sundays and Public Holidays declared by the State Bank of India

1.1.21 **“Working Days”**: All other days except “Non-working Days”.

1.1.22 “**Concurrent use**r” connections are the number of concurrent user requests submission to the system at a point of time

1.1.23 “**Go-Live**”: The system will be considered as “Live” based on the criteria defined in this RFP.

1.1.24 “**24*7**” is defined as three shifts of 8 hours every day. This is applicable for all seven days of the week without any non-working days

1.1.25 “**Scheduled Maintenance Time**” is defined as the time that the System is not in service due to a scheduled activity as defined in this SLA. The scheduled maintenance time would not be during the 16x7 (7:00 am to 11:00 pm) timeframe. Furthermore, scheduled maintenance time is planned downtime taken after permission of the SBI.

1.1.26 “**Scheduled operation time**” is defined as the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time. The total operation time for the systems and applications within the Primary DC, DR, will be 24x7x365 (per year).

1.1.27 “**System or Application downtime**” is defined as the accumulated time during which the System is totally inoperable within the Scheduled Operation Time but outside the scheduled maintenance time. It is measured from the time a call is logged with the AP of the failure or the failure is known to the AP from the availability measurement tools to the time when the System is returned to proper operation.

1.1.28 "**Availability**" refers to the time for which the services and facilities are available for conducting operations on the system including application and associated infrastructure. Availability is defined as: {(Scheduled Operation Time – System Downtime)/ (Scheduled Operation Time)} * 100%

1.1.29 "**Incident**" refers to any event/abnormalities in the functioning of the any of IT equipment/services that may lead to disruption in normal operations of the Data Centre, system or application services.

1.1.30 Terminologies utilized in this RFP are clarified in the following points

1.1.31 "System" as mentioned in this RFP refers to the ALP Application

1.1.32 "Administrator" as mentioned in this RFP refers to the "System Administrator"

1.2 Interpretations:

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

1.2.2 The singular includes the plural and vice versa.

1.2.3 Reference to any gender includes each other gender.

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

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

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

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

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

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

1.3 Commencement, Term & Change in Terms

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

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

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

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

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

3.4 Payments

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

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

[7] Please determine the applicability of the taxes.

the Bank through a credit note or revised invoices. In case Service Provider fails to issue credit note/ revised invoice, the Bank shall have right to withhold the payment or set-off penal amount from current invoices.

3.5 Bank Guarantee and Penalties

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

3.5.2 The Bank Guarantee is required to protect the interest of the Bank against 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/ liquidated damages 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) The service provider shall comply with all the applicable laws, regulations, and regulatory directions issued by the Reserve Bank of India (RBI) and other competent authorities in relation to data storage, localisation and processing, including but not limited to the RBI Master Direction on Outsourcing of Information Technology services (2023) and the RBI circular on storage of Payment System Data (2018) as amended from time to time.

(i) The service provider shall not erase, delete, purge, revoke access to, or otherwise make unavailable, any data belonging to the bank or its customers, whether stored, processed, or transmitted as part of services, without the Bank's prior written approval. All actions relating to data modification, erasure, or destructions shall be carried out only under written instruction of the Bank and in accordance with (a) the bank's data retention and destruction policies; (b) regulatory directions issued by the Reserve Bank of India (RBI) or any competent authority.

(j) Service provider shall ensure that storage of data only in India as per the extant regulatory requirements

(k) 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.

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

(m) 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.

(n) The service Provider shall identify, document, and maintain a list of skilled resources (key personnel, technical specialist) who provide core services under this Agreement. These persons shall be designated as "Essential Personnel". The service provider shall ensure: (a) back-up arrangements are in place for such essential personnel. (b) The service provider shall maintain knowledge transfer, cross-training, and succession plans to ensure continuity in case of absence, leave, incapacity, or other unavailability of any essential personnel. In situations of exigency (including but not limited to pandemics, natural disasters, infrastructure disruptions, regulatory restrictions), the service provider shall ensure that a limited number of essential personnel are able to work on -site at locations during exigencies.

(o) Software Bill of Materials (SBOM)

All the software supplied to the Bank or developed for the Bank must be accompanied by a complete SBOM. The SBOM of the software supplied to the Bank or developed for the Bank must include the data fields contained in the **Annexure-I** of this document. In addition, the Software OEM/Owner/Vendor must ensure that:

- The Software supplied to the Bank or developed for the Bank is having a complete SBOM including all the dependencies up to the last level.
- Software OEM/Owner/Vendor should design a Vulnerability Exchange Document (VEX) after a vulnerability is discovered informing the bank about the exploitability status to help prioritize the remediation efforts.

Subsequently, Software OEM/Owner/Vendor should provide the Common Security Advisory Framework (CSAF) advisory, which includes detailed information about the vulnerability, such as a description, affected product versions, severity assessment, recommended mitigation steps etc.

- Software OEM/Owner/Vendor will ensure update of the SBOM in case of any version update or any change in the details on the data point in the SBOM for any reason whatsoever.
- The service provider shall ensure suitable back-to-back arrangements with OEM.

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

(q) The service provider shall ensure adherence to Prevention of Money Laundering Act, 2002 and other applicable AML/CFT laws. The service provider shall provide, as and when required by the Bank, copies of AML policy and other related documents.

(r) ____________*<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 _____one (1) year_______ (Term) from the date of acceptance.

5.2 Any defect found will be evaluated mutually to establish the exact cause of the defect.

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 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 Rs.___________ on demand to the Bank, which may be settled from the payment of invoices or bank guarantee for the contracted period. Transition & Knowledge Transfer plan is mentioned in **Annexure 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 ____% of total Project cost for delay of each week or part thereof maximum up to ___% of total Project cost. Once the maximum deduction is reached, the Bank may consider termination of the Agreement.

10. RELATIONSHIP BETWEEN THE PARTIES

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

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

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

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

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

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

11. SUB CONTRACTING

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

12. INTELLECTUAL PROPERTY RIGHTS

12.1 For any technology / Software / solution developed/used/supplied by Service provider for performing Services or licensing and implementing Software and solution for the Bank as part of this Agreement, 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.

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

12.3 Subject to below mentioned sub-clause 12.4 and 12.5 of this Agreement, Service Provider shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the Bank against all 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 Agreement.

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

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

12.6 Service provider hereby grants the Bank a *fully paid-up, irrevocable, unlimited, perpetual, non-exclusive/exclusive license* throughout the territory of India or abroad to access, replicate, modify and use Software licensed/developed including its upgraded versions available during the term of this Agreement by Service provider as part of this engagement, including all inventions, designs and trademarks embodied therein perpetually.

12.7 Software licensed/developed as part of this Agreement can be put to use in all offices of the Bank.

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 the Bank reserves the right to audit the service provider, annual or as applicable, 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. SOURCE CODE ESCROW AGREEMENT[9]

17.1 Service Provider shall deposit the source code of the Software and everything required to independently maintain the Software, to the source code escrow account and agrees to everything mentioned in source code escrow agreement.

17.2 Service provider shall deposit the latest version of source code in escrow account at regular intervals as mentioned in source code escrow agreement.

17.3 The Bank shall have the right to get the source code released and will receive no opposition/hindrances from the escrow agent and Service provider under the following conditions:-

(i) In the event wherein Service provider files a voluntary petition in bankruptcy or insolvency or has been otherwise declared Insolvent/Bankrupt; or

(ii) In the event wherein Service provider has declared its expressed/written unwillingness to fulfill his contractual obligations under this Agreement; or

(iii) Service Provider is wound up, or ordered wound up, or has a winding up petition ordered against it, or assigns all or a substantial part of its business or assets for the benefit of creditors, or permits the appointment of a receiver for the whole or substantial part of its business or assets, or otherwise ceases to conduct its business in the normal course; or

(iv) Service Provider discontinues business because of insolvency or bankruptcy, and no successor assumes Service Provider's Software maintenance obligations or obligations mentioned in the Agreement; or

(v) Service Provider dissolves or ceases to function as a going concern or to conduct its operation in the normal course of business or intends and conveys its intention to do so; or

(vi) Any other release condition as specified in source code escrow agreement.

[9] This agreement is to be made wherein ownership over the Software is not provided. The user department has to delete inapplicable para from clause 16 (Ownership and Escrow Agreement).

17.4 Service provider agrees to bear the payment of fees due to the escrow agent.

17.5 The escrow agreement shall ipso-facto would get terminated on delivery of source code to either of the parties upon the terms & conditions mentioned in source code escrow agreement.

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:

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

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

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

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

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

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;

(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,

[10] Please see Clause 12 ‘IPR Indemnification’

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

____

____

____

(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 < *Strike of whichever is inapplicable*>.

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.

25.11

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 per the Scope defined in the RFP

ANNEXURE-B

INFRASTUCTURE MANAGEMENT METRICS

As defined in the RFP

ANNEXURE-C

APPLICATION DEVELOPMENT & MAINTENANCE METRIC.

Impact Level	Description/Measure	Response Time	Resolution Time
Level 1	Low impact	*<to be filled in by the concerned dept. depending on the criticality of service>*	*<to be filled in by the concerned dept. depending on the criticality of service>*
Level 2	Medium impact	*<to be filled in by the concerned dept. depending on the criticality of service>*	*<to be filled in by the concerned dept. depending on the criticality of service>*
....	....		
Level.....	Highest impact	*<to be filled in by the concerned dept. depending on the criticality of service>*	*<to be filled in by the concerned dept. depending on the criticality of service>*

Urgency Level	Description/Measure	Response time	Resolution time
Level 1		*<to be filled in by the concerned dept. depending on the criticality of service>*	*<to be filled in by the concerned dept. depending on the criticality of service>*
Level 2		*<to be filled in by the concerned dept. depending on the criticality of service>*	*<to be filled in by the concerned dept. depending on the criticality of service>*
....			
Level.....	To be performed on top priority	*<to be filled in by the concerned dept. depending on the criticality of service>*	*<to be filled in by the concerned dept. depending on the criticality of service>*

<Priorities areto be filled in by the concerned dept. depending on the criticality of service>

IMPACT	Urgency Level				
		Level 1	Level 2		Level n
	Level 1	Priority A	Priority A		Priority C
	Level 2	Priority A	Priority B		Priority D
	....		Priority J	Priority K	Priority L
	Level.....	Priority L	Priority M	Priority N	Priority O

ANNEXURE-D

SERVICE DESK SUPPORT METRIC*<strike off if not applicable>*

SL no.	Service level category	Service level object	Measurement range/criteria
1.	Call type level 1, *<strike off which ever in not applicable>*	<……………….(requirement)/ call escalated by sbi service desk to ……………service provider's team>*<strike off which ever in not applicable>*	<…………………>*<to be filled in by the concerned dept. depending on the criticality of service>*
	Call type level 12, *<strike off which ever in not applicable>*	<……………….(requirement)/ call escalated by sbi service desk to ……………service provider's team>*<strike off which ever in not applicable>*	<…………………>*<to be filled in by the concerned dept. depending on the criticality of service>*

SERVICE LEVEL REPORTING/ FREQUENCY[11]*<strike off if not applicable>*

<Describe the service level reporting frequency and methodology>

Report Name	Interval	Recipient	Responsible

SERVICE REVIEW MEETING[12]*<strike off if not applicable>*

Service Review meeting shall be held annually/ half yearly. The following comprise of the Service Review Board:

- President,
- Members…………….

[11] The purpose of this section is to document reports used to measure service levels. These reports must align with the service measurement and should support these measurements.

[12] The purpose of this section to describe the frequency of meeting and composition of service review board.

ANNEXURE-E

ESCALATION MATRICS[13]*<strike off if not applicable>*

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.>*			

[13] 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

<Under mentioned are proposed penalty metrics, they are required to be customized by the concerned dept.><strike off whichever is not applicable>

PENALTY FOR NON PERFORMANCE OF SLA

Service level category	**SLA Measure**	**Penalty Calculation**
Application Uptime/Downtime/ RTO/RPO *<strike off whichever is not applicable>*	*<delay in minutes / hours /days>< to be provided by the dept.>*	
Delivery Schedule	*<Delay (in working days)>< to be provided>*	
Installation	*<delay in minutes / hours /days>< to be provided by the dept.>*	
User Acceptance Testing	*<delay in minutes / hours /days>< to be provided by the dept.>*	
Live in Production	*<delay in minutes / hours /days>< to be provided by the dept.>*	
Periodical training	*<Delay (in working days)>< to be provided>*	*………<For each resource not trained>*
Source Code	*<Delay (in working days)>< to be provided>*	
Non-availability of staff		
Reports/		

PENALTY FOR EVERY ITEMS, Penalty at the rates given below:

Category of defect	**Service Area**	**Penalty**
Minor		
Medium		
Major		
Critical		

PENALTY FOR NON PERFORMANCE AT HELP DESK

Service Area	**SLA measurement**	**Penalty % on ___________** *<to be provided by the dept.,>*		**Calculate penalty on**
		0 %	**______% (for every 1% shortfall from the stipulated service level**	
Help Desk	Time taken for resolution of calls (99.9% of the calls should be resolved within the stipulated response time)	More than or equal to 99.9 % of service level	Less than 99.9 % of service level	*<to be provided by the dept.,>*

ANNEXURE G

Transition & Knowledge Transfer Plan

1. Introduction

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

2. Objectives

2.1 The objectives of this annexure are to:

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

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

(3) ensure that all relevant Assets are transferred.

3. General

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

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

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

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

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

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

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

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

(2) where any support and materials necessary to undertake the transfer work or any costs incurred by Service Provider are additional to those in place as part

of the proper provision of the Services the Bank shall pay Service Provider for staff time agreed in advance at the rates agreed between the parties and for materials and other costs at a reasonable price which shall be agreed with the Bank.

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

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

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

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

3.6 Service Provider shall provide such information as the Bank reasonably considers to be necessary for the actual Replacement SERVICE PROVIDER, or any potential Replacement SERVICE PROVIDER during any procurement process, to define the tasks which would need to be undertaken in order to ensure the smooth transition of all or any part of the Services.

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

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

4. Replacement SERVICE PROVIDER

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

5. Subcontractors

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

6. Transfer of Configuration Management Database

6.1 6 (six) months prior to expiry or within 2 (two) week of notice of termination of this Agreement Service Provider shall deliver to the Bank a full, accurate and up to date cut of content from the Configuration Management Database (or equivalent) used to store details of Configurable Items and Configuration Management data for all products used to support delivery of the Services.

7. Transfer of Assets

7.1 6 (six) months prior to expiry or 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

9.1 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

10.1 6 (six) months prior to expiry or within 2 (two) weeks of notice of termination of this Agreement Service Provider shall deliver to the Bank a 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

11.1 6 (six) months prior to expiry or within 2 (two) weeks of notice of termination of this Agreement Service Provider shall deliver to the Bank:

(a) a plan for the handover and continuous delivery of the Service Desk function and allocate the required resources;

(b) full and up to date, both historical and outstanding Service Desk ticket data including, but not limited to:

(1) Incidents;

(2) Problems;

(3) Service Requests;

(4) Changes;

(5) Service Level reporting data;

(c) a list and topology of all tools and products associated with the provision of the Software and the Services;

(d) full content of software builds and server configuration details for software deployment and management; and

(e) monitoring software tools and configuration.

12. Transfer of Knowledge Base

12.1 6 (six) months prior to expiry or within 2 (two) week of notice of termination of this Agreement Service Provider shall deliver to the Bank a full, accurate and up to date cut of content from the knowledge base (or equivalent) used to troubleshoot issues arising with the Services but shall not be required to provide information or material which Service Provider may not disclose as a matter of law.

13. Transfer of Service Structure

13.1 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

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		

S. No	Controls to be implemented		Compliance (Yes / No)	If under implementation, give date by which implementation will be done
		g. Personnel Security		
		h. Physical Security		
		i. Internal security assessment processes		
3	Whether a proper documented Change Management process has been instituted by the Processor?			
4	Whether the Processor has a documented policy and process of Incident management /response?			
5	Whether the Processor's environment is suitably protected from external threats by way of:	a. Firewall		
		b. WAF		
		c. IDS/IPS		
		d. AD		
		e. AV		
		f. NAC		
		g. DLP		
		h. Any other technology		
6	Whether rules are implemented on Firewalls of the Processor environment as per an approved process?			
7	Whether firewall rule position is regularly monitored for presence of any vulnerable open port or any-any rule?			
8	Whether proper log generation, storage, management and analysis happens for the Processor application?			
9	Is the Processor maintaining all logs for forensic readiness related to:	a. Web		
		b. Application		
		c. DB		
		d. Configuration		
		e. User access		
10	Whether the Processor maintains logs for privileged access to their critical systems?			
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?			

S. No	Controls to be implemented		Compliance (Yes / No)	If under implementation, give date by which implementation will be done
13	Whether the Processor environment is segregated into militarized zone (MZ) and demilitarized zone (DMZ) separated by Firewall, where any access from an external entity is permitted through DMZ only?			
14	Whether Processor has deployed secure environments for their applications for:	a. Production		
		b. Disaster recovery		
		c. Testing environments		
15	Whether the Processor follows the best practices of creation of separate network zones (VLAN Segments) for:	a. Web		
		b. App		
		c. DB		
		d. Critical applications		
		e. Non-Critical applications		
		f. UAT		
16	Whether the Processor configures access to officials based on a documented and approved Role Conflict Matrix?			
17	Whether Internet access is permitted on:	a. Internal servers		
		b. Database servers		
		c. Any other servers		
18	Whether the Processor has deployed a dedicated information security team independent of IT, reporting directly to MD/CIO for conducting security related functions & operations?			
19	Whether CERT-IN Empaneled ISSPs are engaged by the third party for ensuring security posture of their application?			
20	Whether quarterly vulnerability assessment and penetration testing is being done by the Processor for their infrastructure?			
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?			

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

S. No	Controls to be implemented		Compliance (Yes / No)	If under implementation, give date by which implementation will be done
36	Whether the selection criteria for awarding the work to Processor vendor is based on the quality of service?			
37	Whether the SLA/agreement between SBI and the Processor contains these clauses:	a. Right to Audit to SBI with scope defined		
		b. Adherence by the vendor to SBI Information Security requirements including regular reviews, change management, port management, patch management, backup management, access management, log management etc.		
		c. Right to recall data by SBI.		
		d. Regulatory and Statutory compliance at vendor site. Special emphasis on section 43A of IT Act 2000 apart from others.		
		e. Availability of Compensation clause in case of any data breach or incident resulting into any type of loss to SBI, due to vendor negligence.		
		f. No Sharing of data with any third party without explicit written permission from competent Information Owner of the Bank including the Law Enforcement Agencies.		

ANNEXURE-I

FORMAT FOR THE SOFTWARE BILL OF MATERIALS (SBOM) OF THE SOFTWARE SUPPLIED TO THE BANK / DEVELOPED FOR THE BANK

Sr.	Data Field	Details
1	Component Name	
2	Component Version	
3	Component Description	
4	Component Supplier	
5	Component License	
6	Component Origin	
7	Component Dependencies	
8	Vulnerabilities	
9	Patch Status	
10	Release Date	
11	End of Life (EOL Date) Date	
12	End of Support (EOS Date) Date	
13	Criticality	
14	Usage Restrictions	
15	Checksums or Hashes	
16	Executable Property	
17	Archive Property	
18	Structured Property	
19	Unique Identifier	
20	Comments or Notes	
21	Any Other Relevant Data	
22	Author of SBOM Data	
23	Timestamp	

Guidance notes on filling the SBOM format above:

1. **Component Name**: The name of the software component or library included in the SBOM.
2. **Component Version**: The version number or identifier of the software component.
3. **Component Description**: A brief description or summary of the functionality and purpose of the software component.
4. **Component Supplier**: The entity or organization that supplied the software component, such as a vendor, third-party supplier, or open-source project.
5. **Component License**: The license under which the software component is distributed, including details such as the license type, terms, and restrictions.
6. **Component Origin**: The source or origin of the software component, such as whether it is proprietary, open-source, or obtained from a third-party vendor.
7. **Component Dependencies**: Any other software components or libraries that the current component depends on, including their names and versions.

8. **Vulnerabilities**: Information about known security vulnerabilities or weaknesses associated with the software component, including severity ratings and references to security advisories or CVE identifiers.
9. **Patch Status**: The patch or update status of the software component, indicating whether any patches or updates are available to address known vulnerabilities or issues.
10. **Release Date**: The date when the software component was released or made available for use.
11. **End-of-Life (EOL) Date**: The date when support or maintenance for the software component is scheduled to end, indicating the end of its lifecycle.
12. **Criticality**: The criticality or importance of the software component to the overall functionality or security of the application, often categorized as critical, high, medium, or low.
13. **Usage Restrictions**: Any usage restrictions or limitations associated with the software component, such as export control restrictions or intellectual property rights.
14. **Checksums or Hashes**: Cryptographic checksums or hashes of the software component files to ensure integrity and authenticity.
15. **Executable Property**: Attributes indicating whether a component within an SBOM can be executed.
16. **Archive Property**: Characteristics denoting if a component within an SBOM is stored as an archive or compressed file.
17. **Structured Property**: Descriptors defining the organized format of data within a component listed in an SBOM.
18. **Unique Identifier**: A unique identifier is a distinct code assigned to each software component, structured as

    "pkg:supplier/OrganizationName/ComponentName@Version?qualifiers&subpath," aiding in tracking ownership changes and version updates, thus ensuring accurate and consistent software component management.
19. **Comments or Notes**: Additional comments, notes, or annotations relevant to the software component or its inclusion in the SBOM.
20. **Any Other Relevant Data:** Any other data related to the component may be incorporate herein. Additional rows may be added, if need be.
21. **Author of SBOM Data**: The name of the entity that creates the SBOM data for this component.
22. **Timestamp**: Record of the date and time of the SBOM data assembly.

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:**

(a) "Confidential Information" means non-public information that Disclosing Party designates as being confidential or which, under the circumstances surrounding disclosure ought to be treated as confidential. "Confidential Information" includes, without limitation, information relating to developed, installed or purchased Disclosing Party software or hardware products, the information relating to general architecture of Disclosing Party's network, information relating to nature and content of data stored within network or in any other storage media, Disclosing Party's business policies, practices, methodology, policy design delivery, and information received from others that Disclosing Party is obligated to treat as confidential. Confidential Information disclosed to Receiving Party by any Disclosing Party Subsidiary and/ or agents is covered by this agreement

(b) Confidential Information shall not include any information that: (i) is or subsequently becomes publicly available without Receiving Party's breach of any obligation owed to Disclosing party; (ii) becomes known to Receiving Party free from any confidentiality obligations prior to Disclosing Party's disclosure of such information to Receiving Party; (iii) became known to Receiving Party from a source other than Disclosing Party other than by the breach of an obligation of confidentiality owed to Disclosing Party and without confidentiality restrictions on use and disclosure; or (iv) is independently developed by Receiving Party.

(c) "Confidential Materials" shall mean all tangible materials containing Confidential Information, including without limitation written or printed documents and computer disks or tapes, whether machine or user readable.

2. **Restrictions**

(a) Each party shall treat as confidential the Contract and any and all information ("confidential information") obtained from the other pursuant to the Contract and shall not divulge such information to any person (except to such party's "Covered Person" which term shall mean employees, contingent workers and professional advisers of a party who need to know the same) without the other party's written consent provided that this clause shall not extend to information which was rightfully in the possession of such party prior to the commencement of the negotiations leading to the Contract, which is already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this clause). Receiving Party will have executed or shall execute appropriate written agreements with Covered Person, sufficient to enable it to comply with all the provisions of this Agreement. If 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.

(b) Receiving Party may disclose Confidential Information in accordance with judicial or other governmental order to the intended recipients (as detailed in this clause), provided Receiving Party shall give Disclosing Party reasonable notice (provided not restricted by applicable laws) prior to such disclosure and shall comply with any applicable protective order or equivalent. The intended recipients for this purpose are:

i. the statutory auditors of the either party and

ii. government or regulatory authorities regulating the affairs of the parties and inspectors and supervisory bodies thereof

(c) Confidential Information and Confidential Material may be disclosed, reproduced, summarized or distributed only in pursuance of Receiving Party's business relationship with Disclosing Party, and only as otherwise provided hereunder. Receiving Party agrees to segregate all such Confidential Material from the confidential material of others in order to prevent mixing.

3. **<u>Rights and Remedies</u>**

(a) Receiving Party shall notify Disclosing Party immediately upon discovery of any unauthorized used or disclosure of Confidential Information and/ or Confidential Materials, or any other breach of this Agreement by Receiving Party, and will cooperate with Disclosing Party in every reasonable way to help Disclosing Party regain possession of the Confidential Information and/ or Confidential Materials and prevent its further unauthorized use.

(b) Receiving Party shall return all originals, copies, reproductions and summaries of Confidential Information or Confidential Materials at Disclosing Party's request, or at Disclosing Party's option, certify destruction of the same.

(c) Receiving Party acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that disclosing party shall be entitled, without waiving any other rights or remedies (including but not limited to as listed below), to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.

i. Suspension of access privileges

ii. Change of personnel assigned to the job

iii. Termination of contract

(d) Disclosing Party may visit Receiving Party's premises, with reasonable prior notice and during normal business hours, to review Receiving Party's compliance with the term of this Agreement.

4. **Miscellaneous**

(a) All Confidential Information and Confidential Materials are and shall remain the sole and of Disclosing Party. By disclosing information to Receiving Party, Disclosing Party does not grant any expressed or implied right to Receiving Party to disclose information under the Disclosing Party's patents, copyrights, trademarks, or trade secret information.

(b) Confidential Information made available is provided "As Is," and disclosing party disclaims all representations, conditions and warranties, express or implied, including, without limitation, representations, conditions or warranties of accuracy, completeness, performance, fitness for a particular purpose, satisfactory quality and merchantability provided same shall not be construed to include fraud or wilful default of disclosing party.

(c) Neither party grants to the other party any license, by implication or otherwise, to use the Confidential Information, other than for the limited purpose of evaluating or advancing a business relationship between the parties, or any license rights whatsoever in any patent, copyright or other intellectual property rights pertaining to the Confidential Information.

(d) The terms of Confidentiality under this Agreement shall not be construed to limit either party's right to independently develop or acquire product without use of the other party's Confidential Information. Further, either party shall be free to use for any purpose the residuals resulting from access to or work with such Confidential Information, provided that such party shall maintain the confidentiality of the Confidential Information as provided herein. The term "residuals" means information in non-tangible form, which may be retained by person who has had access to the Confidential Information, including ideas, concepts, know-how or techniques contained therein. Neither party shall have any obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of residuals. However, the foregoing shall not be deemed to grant to either party a license under the other party's copyrights or patents.

(e) This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. It shall not be modified except by a written agreement dated subsequently to the date of this Agreement and signed by both parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of Disclosing Party, its agents, or employees, except by an instrument in writing signed by an authorized officer of Disclosing Party. No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.

(f) . This Agreement shall be governed by and construed in accordance with the laws of Republic of India. Each Party hereby irrevocably submits to the exclusive jurisdiction of the courts of Mumbai.

(g) Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the parties, their successors and assigns.

(h) If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect.

(i) The Agreement shall be effective from _______ ("Effective Date") and shall be valid for a period of ________ year(s) thereafter (the "Agreement Term"). The foregoing obligations as to confidentiality shall survive the term of this Agreement and for a period of five (5) years thereafter provided confidentiality obligations with respect to individually identifiable information, customer's data of Parties or software in human-readable form (e.g., source code) shall survive in perpetuity.

5. **Suggestions and Feedback**

Either party from time to time may provide suggestions, comments or other feedback to the other party with respect to Confidential Information provided originally by the other party (hereinafter "feedback"). Both party agree that all Feedback is and shall be entirely voluntary and shall not in absence of separate agreement, create any confidentially obligation for the receiving party. However, the Receiving Party shall not disclose the source of any feedback without the providing party's consent. Feedback shall be clearly designated as such and, except as otherwise provided herein, each party shall be free to disclose and use such Feedback as it sees fit, entirely without obligation of any kind to other party. The foregoing shall not, however, affect either party's obligations hereunder with respect to Confidential Information of other party.

Dated this __________ day of _______ (Month) *20*__ at __________(place)

For and on behalf of ___________________________

Name		
Designation		

Place		
Signature		

For and on behalf of ____________________________

Name		
Designation		
Place		
Signature		

Appendix-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

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	
Start Date	
End Date	
Current Status (In Progress / Completed)	
Size of Project	
Value of Work Order (In Lakh) (only single work order)	

Name & Signature of authorised signatory

Seal of Company

Appendix-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 :

- 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 financial Bid and before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the BUYER or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

2.8 The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, Bid evaluation, contracting and implementation of the contract.

2.9 The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

2.10 The BIDDER shall not use improperly, for purposes of competition or personal gain, or pass. on 'to° others, any -information provided by the BUYER as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.

2.11 The BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

2.12 The BIDDER shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

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

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

3. **Previous Transgression**

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

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

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

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

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

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

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

5. Sanctions for Violations

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

(i) To immediately call off the pre contract negotiations without assigning any reason and without giving any compensation to the BIDDER. However, the proceedings with the other BIDDER(s) would continue, unless the BUYER desires to drop the entire process.

(ii) The Earnest Money Deposit (in pre-contract stage) and/or Security Deposit/Performance Bond (after the contract is signed) shall stand forfeited either fully or partially, as decided by the BUYER and the BUYER shall not be required to assign any reason therefore.

(iii) To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER.

(iv) To recover all sums already paid by the BUYER, and in case of an Indian BIDDER with interest thereon at 2% higher than the prevailing Base Rate of State Bank of India, while in case of a BIDDER from a country other than India with interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the BIDDER from the BUYER in connection with any other contract for any other stores, such outstanding could also be utilized to recover the aforesaid sum and interest.

(v) To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the BIDDER, in order to recover the payments, already made by the BUYER, along with interest.

(vi) To cancel all or any other Contracts with the BIDDER. The BIDDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER.

(vii) To debar the BIDDER from participating in future bidding processes of the BUYER or any of its Subsidiaries for a minimum period of five years, which may be further extended at the discretion of the BUYER.

(viii) To recover all sums paid, in violation of this Pact, by BIDDER(s) to any middleman or agent or broker with a view to securing the contract.

(ix) Forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

(x) Intimate to the CVC, IBA, RBI, as the BUYER deemed fit the details of such events for appropriate action by such authorities.

5.2 The BUYER will be entitled to take all or any of the actions mentioned at para 5.1(i) to (x) of this Pact also on the Commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defined in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

5.3 The decision of the BUYER to the effect that a breach of the provisions of this Pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the Independent Monitor(s) appointed for the purposes of this Pact.

6. Fall Clause

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

7. Independent Monitors

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

Name	Shri Satyajit Mohanty	Smt. Rashmi Verma
Designation	IPS (Retd.)	IAS (Retd.)
Email ID	satyajitmohanty88@gmail.com	rashmi.naveenverma@gmail.com

7.2 The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.

7.3 The Monitors shall not be subjected to instructions by the representatives of the parties and perform their functions neutrally and independently.

7.4 Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings. Parties signing this Pact shall not approach the Courts while representing the matters to Independent External Monitors and he/she will await their decision in the matter.

7.5 As soon as the Monitor notices, or has reason to believe, a violation of this Pact, he will so inform the Authority designated by the BUYER.

7.6 The BIDDER(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the BIDDER. The BIDDER will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractor(s) with confidentiality.

7.7 The BUYER will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the parties. The parties will offer to the Monitor the option to participate in such meetings.

7.8 The Monitor will submit a written report to the designated Authority of BUYER/Secretary in the Department/ within 8 to 10 weeks from the date of reference or intimation to him by the BUYER / BIDDER and, should the occasion arise, submit proposals for correcting problematic situations.

8. Facilitation of Investigation

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

9. Law and Place of Jurisdiction

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

10. Other Legal Actions

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

11. Validity

11.1 The validity of this Integrity Pact shall be from date of its signing and extend upto 5 years or the complete execution of the contract to the satisfaction of both the BUYER and the BIDDER/Seller, including warranty period, whichever is later. In case BIDDER is unsuccessful, this Integrity Pact shall expire after six months from the date of the signing of the contract, with the successful Bidder by the BUYER.

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

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

For BUYER	For BIDDER
Name of the Officer.	Chief Executive Officer/
Designation	Authorised Signatory
Office / Department / Branch	Designation
State Bank of India.	
Witness	Witness
1	
	1.
2	
	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 ALP/ SERVICES TO STATE BANK OF INDIA TO MEET SUCH REQUIRMENT AND PROVIDE SUCH SOFTWARE ALP/ SERVICES AS ARE SET OUT IN THE SBI:RMD/PRMD/2025-26/01 dated 02.01.2026

WHEREAS State Bank of India (SBI), having its Corporate Office at Nariman Point, Mumbai, and Regional offices at other State capital cities in India has invited Request for Proposal to develop, implement and support ________________(name of Software ALP/ Service) as are set out in the Request for Proposal **SBI:RMD/PRMD/2025-26/01** dated **02.01.2026**.

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

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

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

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

a) Any forbearance or commission on the part of the SBI in enforcing the conditions of the said agreement or in compliance with any of the terms and conditions stipulated in the said Bid and/or hereunder or granting of any time or showing of any indulgence by the SBI to the Bidder or any other matter in connection therewith shall not discharge us in any way our obligation under this guarantee. This guarantee shall be discharged only by the performance of the Bidder of their obligations and in the event of their failure to do so, by payment by us of the sum not exceeding Rs.__________/- (Rupees ______________________ Only)

b) Our liability under these presents shall not exceed the sum of Rs.__________/- (Rupees ______________________ Only)

c) Our liability under this agreement shall not be affected by any infirmity or irregularity on the part of our said constituents in tendering for the said work or their obligations there under or by disALP or change in the constitution of our said constituents.

d) This guarantee shall remain in force upto 180 days provided that if so desired by the SBI, this guarantee shall be renewed for a further period as may be indicated by them on the same terms and conditions as contained herein.

e) Our liability under this presents will terminate unless these presents are renewed as provided herein upto 180 days or on the day when our said constituents comply with their obligations, as to which a certificate in writing by the SBI alone is the conclusive proof, whichever date is earlier.

f) Unless a claim or suit or action is filed against us on or before____(date to be filled by BG issuing bank), all the rights of the SBI against us under this guarantee shall be forfeited and we shall be released and discharged from all our obligations and liabilities hereunder.

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

Notwithstanding anything contained hereinabove:

(a) Our liability under this Bank Guarantee shall not exceed Rs………….……./- (Rupees …………………….only)

(b) This Bank Guarantee shall be valid upto ………………………

(c) We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before ……………………

Yours faithfully,

For and on behalf of

____

Authorized official of the bank

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

Appendix-Q: DATA PROCESSING AGREEMENT

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

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

And

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

WHEREAS:

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

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

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

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

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation:

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

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

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

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

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

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

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

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

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

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

1.1.10 "EEA" means the European Economic Area.

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

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

1.1.13 "Data Transfer" means:

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

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

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

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

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

1.1.17 “Personnel” means the personnel of the Processor, Subcontractors and 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. aThe Bankt 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:	j. Business Continuity Management		
		k. Backup management		
		l. Desktop/system/server/network device hardening with baseline controls		
		m. Patch Management		
		n. Port Management Media Movement		

S. No	Controls to be implemented		Compliance (Yes / No)	If under implementation, give date by which implementation will be done
		o. Log Management		
		p. Personnel Security		
		q. Physical Security		
		r. 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:	i. Firewall		
		j. WAF		
		k. IDS/IPS		
		l. AD		
		m. AV		
		n. NAC		
		o. DLP		
		p. 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:	f. Web		
		g. Application		
		h. DB		
		i. Configuration		
		j. 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?			

S. No	Controls to be implemented		Compliance (Yes / No)	If under implementation, give date by which implementation will be done
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:	d. Production		
		e. Disaster recovery		
		f. Testing environments		
15	Whether the Processor follows the best practices of creation of separate network zones (VLAN Segments) for:	g. Web		
		h. App		
		i. DB		
		j. Critical applications		
		k. Non-Critical applications		
		l. 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:	d. Internal servers		
		e. Database servers		
		f. Any other servers		
18	Whether the Processor has deployed a dedicated information security team independent of IT, reporting directly to MD/CIO for conducting security related functions & operations?			
19	Whether CERT-IN Empaneled ISSPs are engaged by the third party for ensuring security posture of their application?			
20	Whether quarterly vulnerability assessment and penetration testing is being done by the Processor for their infrastructure?			

S. No	Controls to be implemented	Compliance (Yes / No)	If under implementation, give date by which implementation will be done
21	Whether suitable Security Certifications (ISO, PCI-DSS etc.) of the security posture at vendor environment are in place?		
22	Whether the Processor has deployed any open source or free software in their environment?		
	If yes, whether security review has been done for such software?		
23	Whether the data shared with the Processor is owned by SBI (SBI = Information Owner)?		
24	Whether the data shared with the Processor is of sensitive nature?		
25	Whether the requirement and the data fields to be stored by the Processor is approved by Information Owner?		
26	Where shared, whether the bare minimum data only is being shared? (Please document the NEED for sharing every data field)		
27	Whether the data to be shared with Processor will be encrypted as per industry best standards with robust key management?		
28	Whether the Processor is required to store the data owned by State Bank?		
29	Whether any data which is permitted to be stored by the Processor will be completely erased after processing by the Processor at their end?		
30	Whether the data shared with the Processor is stored with encryption (Data at rest encryption)?		
31	Whether the data storage technology (Servers /Public Cloud/ Tapes etc.) has been appropriately reviewed by IT AO?		
32	Whether the Processor is required to share SBI specific data to any other party for any purpose?		
33	Whether a system of obtaining approval by the Processor from the IT Application Owner is put in place before carrying out any changes?		
34	Whether Processor is permitted to take any crucial decisions on behalf of SBI without written approval from IT Application Owner?		
	If not, are such instances being monitored? IT Application Owner to describe the system of monitoring such instances.		

S. No	Controls to be implemented		Compliance (Yes / No)	If under implementation , give date by which implementation will be done
35	Whether Application Owner has verified that the Processor has implemented efficient and sufficient preventive controls to protect SBI's interests against any damage under section 43 of IT Act?			
36	Whether the selection criteria for awarding the work to Processor vendor is based on the quality of service?			
37	Whether the SLA/agreement between SBI and the Processor contains these clauses:	g. Right to Audit to SBI with scope defined		
		h. 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.		
		i. Right to recall data by SBI.		
		j. Regulatory and Statutory compliance at vendor site. Special emphasis on section 43A of IT Act 2000 apart from others.		
		k. Availability of Compensation clause in case of any data breach or incident resulting into any type of loss to SBI, due to vendor negligence.		
		l. No Sharing of data with any third party without explicit written permission from competent Information Owner of the Bank		

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

Appendix-R : SBOM

FORMAT FOR THE SOFTWARE BILL OF MATERIALS (SBOM) OF THE SOFTWARE SUPPLIED TO THE BANK / DEVELOPED FOR THE BANK

Sr.	Data Field	Details
1	Component Name	
2	Component Version	
3	Component Description	
4	Component Supplier	
5	Component License	
6	Component Origin	
7	Component Dependencies	
8	Vulnerabilities	
9	Patch Status	
10	Release Date	
11	End of Life (EOL Date) Date	
12	End of Support (EOS) Date	
13	Criticality	
13	Usage Restrictions	
15	Checksums or Hashes	
16	Executable Property	
17	Archive Property	
18	Structured Property	
19	Unique Identifier	
20	Comments or Notes	
21	Any Other Relevant Data	
22	Author of SBOM Data	
22	Timestamp	

Guidance notes on filling the SBOM format above:

23. **Component Name**: The name of the software component or library included in the SBOM.
24. **Component Version**: The version number or identifier of the software component.
25. **Component Description**: A brief description or summary of the functionality and purpose of the software component.
26. **Component Supplier**: The entity or organization that supplied the software component, such as a vendor, third-party supplier, or open-source project.
27. **Component License**: The license under which the software component is distributed, including details such as the license type, terms, and restrictions.
28. **Component Origin**: The source or origin of the software component, such as whether it is proprietary, open-source, or obtained from a third-party vendor.
29. **Component Dependencies**: Any other software components or libraries that the current component depends on, including their names and versions.
30. **Vulnerabilities**: Information about known security vulnerabilities or weaknesses associated with the software component, including severity ratings and references

to security advisories or CVE identifiers.

31. **Patch Status**: The patch or update status of the software component, indicating whether any patches or updates are available to address known vulnerabilities or issues.
32. **Release Date**: The date when the software component was released or made available for use.
33. **End-of-Life (EOL) Date**: The date when support or maintenance for the software component is scheduled to end, indicating the end of its lifecycle.
34. **Criticality**: The criticality or importance of the software component to the overall functionality or security of the application, often categorized as critical, high, medium, or low.
35. **Usage Restrictions**: Any usage restrictions or limitations associated with the software component, such as export control restrictions or intellectual property rights.
36. **Checksums or Hashes**: Cryptographic checksums or hashes of the software component files to ensure integrity and authenticity.
37. **Executable Property**: Attributes indicating whether a component within an SBOM can be executed.
38. **Archive Property**: Characteristics denoting if a component within an SBOM is stored as an archive or compressed file.
39. **Structured Property**: Descriptors defining the organized format of data within a component listed in an SBOM.
40. **Unique Identifier**: A unique identifier is a distinct code assigned to each software component, structured as

    "pkg:supplier/OrganizationName/ComponentName@Version?qualifiers&subpath," aiding in tracking ownership changes and version updates, thus ensuring accurate and consistent software component management.
41. **Comments or Notes**: Additional comments, notes, or annotations relevant to the software component or its inclusion in the SBOM.
42. **Any Other Relevant Data:** Any other data related to the component may be incorporate herein. Additional rows may be added, if need be.
43. **Author of SBOM Data**: The name of the entity that creates the SBOM data for this component.
44. **Timestamp**: Record of the date and time of the SBOM data assembly.

Appendix- S :MAF

MANUFACTURERS' AUTHORIZATION FORM

No. Date:

To:
(Name and address of Procuring Office)

Dear Sir:

Ref: RFP No. SBI:RMD/PRMD/2025-26/01 dated 02.01.2026

We, who are established and reputable 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.

2. 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 (Warranty/ AMC) 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/Services or out of service due to any reasons, then we shall either provide ourselves or make alternative arrangement for the Warranty/ Service/AMC 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.

3. We also undertake to provide any or all of the following materials, notifications, and information pertaining to the Products supplied by the ABP:

(a) 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

(b) In the event of termination of production of such Products:

i. advance notification to the Bank of the pending termination, in sufficient time to permit the Bank to procure needed requirements; and

ii. following such termination, furnishing at no cost to the Bank, operations manuals, standards and specifications of the Products, if requested.

4. We duly authorise the said ABP to act on our behalf in fulfilling all installations, Technical support and maintenance obligations required by the contract.

5. 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 Manufacturer / Producer)

Note: This letter of authority should be on the letterhead of the manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer. The Bidder in its Bid should include it.

Appendix-T: Cyber security requirements

Cyber Security

1.1 Secure Design:

a. Develop, implement, maintain, and use best in class industry proven security controls that prevents the misuse of information systems and appropriately protect the confidentiality, integrity, and availability of information systems. Follow industry standards such as OWASP, SANS, NIST frameworks during design and development phase.

b. The platform should support strong authentication controls like multifactor authentication

c. The platform should have strong authorization controls. Solution to have controls for prevention against unauthorized data access and distribution. User and admin access control management to be provided as part of solution. Access control to be based on least access privilege principle. <Organization> or team assigned by <Organization> will be reviewing all access controls mechanism defined.

d. The solution should be capable of integrating with the existing single sign on facility of the <organization>.

e. While developing the interfaces, the Bidder must ensure and incorporate all necessary security and control features within the application, OS, database, network etc., as per OWASP, SANS standards so as to maintain confidentiality~~,~~ integrity, and availability of the data.

f. Wherever applicable, the solution to have strong file level validation controls for size, type, and content. There should be preventive control against malware. Files should be scanned for any malicious content in a controlled sa~~n~~dbox environment.

g. The file store locations need to be secured. Strong cryptographic controls to be supported. Such controls should be compliant per Industry standards such as FIPS-140, level 2 or higher. 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 scas per NIST framework.

h. Design and Processes of Bidder's Application architecture should support and not limit the bank's applications' security capabilities.

1.2 Secure Development:

a. The solution should adhere to the S-SDLC (Secure System Development Lifecycle) process and practices as per <organization> IS policy.

b. Bidder 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 <organization>

c. Developers should be skilled in secure coding and implementing mitigation controls to deal with OWASP Top ten vulnerabilities.

d. Code should be developed as per secure coding practices and reviewed to ensure the same.

1.3 Secure Deployment:

a. The solution for sandbox type environment should be isolated from production environment where data originating from external source could be processed & validated for any malicious content/code before being sent to internal system.

b. All the hardware or required components should be shipped directly from OEM to <organization> premises.

c. Bidder should enforce process and policies such that only authorized users should have access to the source code.

d. Test data shall be selected carefully and protected and controlled.

e. The source code should be maintained in version-controlled environment that provides for logging and audit of all activities performed on source code.

f. Development, test, staging and production environment must be physically and logically separated from one another as far as possible.

g. 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.

h. All the underlying infrastructure components such as OS, servers (web, application, and database) or any product should be hardened on each environment before being made functional.

i. Logging should be defined properly so that in the eventuality of the application being targeted or even compromised it is important for the organization to be able to carry out forensics of the attack as part of its incidence response framework.

j. Bidder should provide support for integration of the application with Web Application Firewall (WAF) and provide the requisite details to WAF Team for implementation of the same.

k. Bidder should provide support for integration of the application with Intrusion Prevention System (IPS) and the requisite details to IPS Team for implementation of the same.

l. The bidder should provide support for integration with SIEM (Security Information and Event Management), DAM (Database Activity Monitoring), and other available tools.

1.4 Security Assessment

a. Howsoever applicable, the bidder to conduct SAST (Static Application Security Testing) & DAST (Dynamic Application Security Testing) and provide detailed reports of the same or <organization> may conduct the SAST. The bidder should close all the vulnerabilities which should be revalidated by conducting SAST & DAST again.

b. The bidder should provide full support to Security Review, VAPT and Risk Assessment of all platforms conducted by <organization>.

c. 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 by First’s Common

Vulnerability Scoring System (CVSS) and Mitre's Common Weakness Enumeration (CWE).

1.5 BCP DR

a. The bidder should have a Business Continuity Plan to ensure continuity of operations through Disaster Recovery mechanisms or alternate procedures, as feasible. Alignment of the same with the Business Continuity Plan of the Bank should be ensured.

b. The selected bidder should develop a disaster recovery plan for restoration of the system in the event of a disaster or major incident. The Disaster Recovery (DR) Plan should be tested prior to the go-live to verify DR readiness. Ensure the promotion of the build to production environment is done in a secure manner and the production environment is ready for the system go-live.

1.6 Secure use of Open Source:

a. The Implementation of open-source technologies should be taken up in compliance with Information Security (IS) policy of the <organization>.

b. The bidder to provide full support in implementation and maintenance for the open-source technologies in terms of upgradation, patching etc.

c. The bidder should provide the list of all open-source libraries being used in the platform. None of these should consist of any malicious code/script. All-such libraries/code should undergo SAST.

d. Developer shall disclose all binary executables (i.e., compiled or byte code; source code is not required) of the software, including all libraries or components.

e. Developer shall disclose the origin of all software and hardware components used in the product including any open source or 3rd party licensed components.

1.7 Security Compliance to Policies and Process:

a. The Bidder shall abide by the access level agreement to ensure safeguards of the confidentiality, integrity, and availability of the information systems. Bidder will not copy any data obtained while performing services under this RFP to any media, including hard drives, flash drives, or other electronic device, other than as expressly approved by <organization>

b. The organization will have the right to audit the bidder's people, processes, technology etc. as part of Vendor security risk assessment process.

c. Solution should also be compliant to Indian Information Technology Act, 2000 (along-with amendments as per Information Technology (Amendment) Act, 2008) and any applicable data privacy & protection Act.

d. The system should be fully compliant with ISO27001 controls.

e. All personnel who will be part of this engagement should agree to the terms and condition of NDA and sign in with the <organization>.

1.8 Security for Support & Maintenance:

a. Bidder should follow all the process defined by <organization> like Incident, Change, Release and Patch Management

b. Static application security testing and dynamic application security testing should be conducted by the bidder for any change request involving a design or code change. All gaps identified will be fixed by Bidder prior to go-live.

c. <organization> reserves the right to conduct further security testing of the source code and the system by either <organization> personnel or another party. Any gaps identified during this testing will be fixed by Bidder at no extra cost to <organization>.

d. Configuration items such as computers and other devices, software & hardware contracts, and licenses, third party tools and business services which are related to the application should be disclosed.

e. Bidder will resolve security incidents as per the agreed SLAs.

f. All user and technical access will be granted as per the Role Based Access Control (RBAC) matrix approved by <organization>. All access will be reviewed as per defined frequency and during control points e.g., when a team-member leave team or organization.

g. Information Security controls will be enforced when moving production data into nonproduction environments e.g., masking sensitive data during the cloning process etc. Audits will be conducted by <organization> to ensure security ~~co~~ntrols sustenance. Any gaps identified will be remediated by the bidder.

h. Bidder shall share the source code of the procured application. In case the source code is not to be shared, the bidder shall provide certificate from regulator approved security auditors, confirming that the code is free from all code related vulnerabilities.

i. Bidder shall ensure compliance with all government, regulatory and Bank's internal security prescriptions, in respect of the product under procurement.

Customer Data Shared for Processing/Storage Offsite			
S. no	**Control**	**Domain**	**Evidence Requirement**
1	Whether third party has implemented physical controls to allow access to computing facilities only to authorized users? If yes, whether the sufficiency and effectiveness of physical controls is assessed by independent security auditors?	Physical Security	ISO27001 certification or any other equivalent Audit Certificate covering the Control Point
2	Whether third party conducts security Assessment of all their applications (SBI related) covering activities	Security Assessment	Evidence of latest CERT In empaneled

	(including not limited to) Appsec, API Testing, Source Code Review, DFRA, Process Review, Access Control, Vulnerability Assessment, Penetration Testing etc. through regulator/ government (CERT empaneled or others) approved auditors. Any device hosted by Third party in SBI environment should also be covered		auditors report along with Scope
3	Whether the 3rd Party/Vendor's Servers are suitably protected from external threats by way of security solutions like firewall, IDS/IPS, AV, DLP etc.?	Network Security	Evidence for controls in place
4	Whether the 3rd Party/Vendor's Endpoints is suitably protected from data exfiltration through Security Solutions like DLP etc.	Network Security	Evidence for controls in place
5	Whether the 3rd Party/Vendor follows the best practices of creation of separate network zones (VLAN segments) for Production and non-Production such as UAT	Network Security	CERT empaneled auditor's Report on verification of its implementation.
6	Whether the Third party periodically monitors/ reviews the firewall rules including that of Open Vulnerable Ports to ensure that only need based rules are in place	Network Security	Approved Process of Firewall Rules and self-certification (signed by IS Head of the company) for non-presence of overly permissible such as Any-Any Rules or generic rules/evidence for latest FW
7	Whether internal servers are exposed to direct Internet access?	Network Security	Evidence of purpose/need of this and verification of controls in place by CERT empanelled auditors.

8	Whether the privilege access activities are logged, (traceable to a specific user id with no default admin or root id used), monitored, controlled, and governed as per best security practices?	Log Management and Monitoring	Evidence of Privileged access logs and PIMS implementation
9	Whether Sufficient logs for Forensic Assessments are generated, stored securely, and reviewed regularly through a SOC	Log Management and Monitoring	Log generation, storage and review process certified by CERT empanelled auditor.
10	Whether the third party has a dedicated Incident Mgmt. Mechanism to handle Cyber Incidents well within the timelines prescribed as per their internal guidelines?	Incident Management	ISO27001 certification or Evidence showing latest Policy Review and Approval
11	Whether resources deployed by third party for development, are properly skilled /trained in Secure Coding Practices, Secure Data management Practises?	Human Resource Security	ISO27001 certification or Undertaking with Evidence covering the control point
12	Whether third party has a mechanism in place to ensure that the employees of third party return the assets containing SBI/SBI Customer data after role change or completion/ termination of the project or company?	Human Resource Security	ISO27001 certification or Asset Mgmt. Procedures Approved, Asset Issue Register
13	Whether employee on-boarding process of third party covers background verification of the officials before allowing access to the systems/ data?	Human Resource Security	ISO27001 certification or Undertaking with evidence covering the control point.
14	Whether the 3rd Party/Vendor/Vendor has (Board/Top Management approved) Information Security Policy and Procedures, in place with periodic reviews (minimum annually) by Top Management? The policy should cover below aspects of Information Security: 1.Human Resource Management 2.Asset Management 3. Cryptographic Controls	Governance	ISO Certification or Content Table/ Page of IS Policy and review history page

	4. Access Management 5. Log Management 6. Third Party Cyber Risk Management 7. Network Security Management 8. Application Security Management 9. End-point Security Management 10. Incident Management 11. Physical Security 12. Change Management		
15	Whether suitable Security certifications (ISO, PCI-DSS, SOC1 and SOC2 etc.) of the security posture at vendor environment are in place?	Governance	Certificate with validity period, if available.
16	Wherever any work or part of work is outsourced by the Third Party to any other party(subletting), whether the Security posture of the subsequent Party(ies) are reviewed to ensure that same are equivalent to those of the third Party (i.e., SBI vendor)?	Governance	SLA Clause and Self Certification of having reviewed the systems of sub-letting entity by vendor i.e., 3rd party.
17	Whether the PII/ SPDI data is secured in transit by encryption with best-in-class encryption standards as per global best practises?	Data Security	Evidence of encryption techniques implemented
18	Whether the key management system of the third party ensures segregation and uniqueness of keys for SBI visà-vis other clients?	Data Security	Approved Process for Key Mgmt. and Evidence of actual implementation of Key Sharing
19	Whether SBI data, stored at 3rd party, is appropriately segregated from other clients at least through logical isolation at database level?	Data Security	Evidence of logical segregation
20	Whether third party has processes in place to permanently erase SBI data from all environments (LIVE/ archived or data in external media), immediately after the need or clearly defined retention period as per the business	Data Security	Self-certification in case of Govt entity and Approved Purging Process & timeline and Evidence of actual implementation for nonGovt entities duly

	engagement? Whether mechanism is in place to monitor the same?		verified by CERT empanelled IS auditor
21	Whether Data at Rest encryption is ensured for both Live and archived data/ backup in external media etc? Are encryption keys sored in HSM	Data Security	Evidence of encryption techniques implemented
22	Whether the third Party has a mechanism to delete all SBI data when consent is revoked by SBI Customer or when the relationship ceases	Data Security	Regulator/ Govt approved or CERT empanelled auditors report on the secured mechanism implemented for deleting the data
23	Whether the application and database (containing SBI data) are hosted in Public Cloud? If yes, whether Cloud Security aspects including but not limited to the following are ensured: - a. Is there a Secure Migration Process b. Is there a Secure Deletion Process c. Is Cloud Security Review performed on regular basis	Cloud Security	(CERT-In/ Govt/ Regulatory approved Auditors report on the Cloud Control checks provided under section “Critical Data Processed or Stored in Multi-tenant Cloud”
24	Whether a properly documented Change Management process has been instituted by the 3rd Party/ Vendor?	Change Management	ISO Certification or Change Management Procedures, Release Trackers
25	Whether the Vendor performs periodic DR Drills	Business Continuity	ISO27001 Certification or Evidence of conducting DR drills, and lessons learnt and their detailed recordings
26	Whether third party has a Patch Management process for all systems is in place and the same is meticulously adhered to as per defined timelines?	Application Security	Evidence of latest patch applied, Patch Mgmt. Procedures
27	Whether the 3rd Party/Vendor configures or provides access to officials based on a documented and approved Role Conflict Matrix?	Access Management	Role Conflict Matrix and evidence of following the same

28	Whether third party permits remote access to internal systems/ applications? If yes whether they are secured by MDM and/or VPN through Hardened Mobile devices like Laptop/ Desktop or Mobiles	Access Management	Evidence for implementation of the Control
29	Whether the Third Party has a Secure Software Development Lifecycle Environment that includes both Software Development and secured usage of Open-Source Tools.	Security Assessment	Regulator/ Govt approved or CERT empanelled auditors report on assessment of the security practices at third party environment
30	Adherence to Continuous Monitoring Clauses in **Appendix E** of this document	Security Posture Maintenance	Relevant evidence for the Control objectives

Appendix U: Exit Management

The AP shall ensure the following:

i. The AP shall prepare and submit structured & detailed transition and exit management plan for approval by the SBI within 6 month post Go-live.

ii. The AP needs to update the transition and exit management on a half yearly basis or earlier in case of major changes during the entire contract duration. This plan needs to be discussed and approved by the SBI.

iii. At the end of the contract period or during the contract period, if any other agency is identified or selected for providing services related to the AP's scope of work, the AP shall ensure that a proper and satisfactory handover is made to the other agency.

iv. All risks during the transition stage shall be properly documented by the AP and mitigation measures shall be planned to ensure a smooth transition without any service disruption.

v. The AP must ensure that no End of Life (EoL) & End of Support (EoS) products (software/hardware) exist at time of transition.

vi. The AP must ensure the latest version of solution or its component are rolled out before the Exit.

vii. In all the cases, the transition and exit management period will start 6 months before the expiration of the contract/exit. The AP will provide shadow support for at least three months and secondary support for an additional three months before the end of the O&M period or termination of the contract, as applicable at no additional cost to the SBI. In case of termination, the exit management period will start from effective date of termination or such other date as may be decided by the SBI but no later than 6 months from effective date of termination.

viii. Closing off all critical open issues as on date of exit; All other open issues as on date of exit shall be listed and provided to the SBI.

ix. The AP shall provide necessary knowledge transfer and transition support. The deliveries are indicated below:

   a. Updated transition plan on a periodic basis.

   b. Complete documentation for the entire system handed over to the SBI/identified agency.

c. Handover of all AMC support related documents, credentials etc. for all OEM products supplied/maintained in the system. Handover MOUs signed for taking services taken from third parties such as digital signature agencies, etc.

d. Handover of the list of complete inventories of all assets created for the project.

e. Assisting the new agency/the SBI with the complete audit of the system including licenses and physical assets.

f. Detailed walk-throughs and demos for the ALP.

g. Hand-over of the entire software including source code, program files, configuration files, setup files, project documentation, user IDs, passwords, security policies, scripts etc.

h. Hand-over of the user IDs, passwords, security policies, scripts etc.

i. Knowledge transfer of the system to the incoming the AP to the satisfaction of the AP per the specified timelines.

x. The AP shall be released from the project once successful transition is completed by meeting the parameters defined for successful transition.

xi. The AP shall ensure that the data, assets, images in the datacenter must be preserved for a period of 6 months from the end of contract. This shall not be deleted/destroyed without the prior consent of the SBI.

xii. The commercial quoted by the Application provider includes transition costs also and SBI will not pay any additional fees for transition.

Appendix V: COTS Solution

Format for Self-declaration of COTS solution

Date:

To,
____
____
____

Dear Sir,

Ref.: RFP No. : SBI:RMD/PRMD/2025-26/01 dated 02.01.2026

This is to certify that COTS Product (s) <product details> proposed as part of the solution is:

1. Readily deployable with or without customization to suit the specific process requirements and does not involve developing the application from scratch or major significant developments in the product; and
2. Implemented by at least 8 organizations < name of the Organizations>; and
3. Implemented and maintained by at least 3 implementation partners <Name of the Implementation Partners> other than the OEM of the COTS Software and each partner have done at least one implementation. At least one of the implementation partners have presence in INDIA.

Signature of authorised official
Name:
Company seal: