REQUEST FOR EXPRESSION OF INTEREST
FOR PROCUREMENT OF THIRD-PARTY LIFECYCLE
MANAGEMENT SYSTEM

Ref: SBI:TPM:CC: EOI:2025-26:01
Dated: 05.12.2025

Vendor Management, Non-IT
Third Party Management Department,
Corporate Centre, Mumbai

Expression of Interest for procurement of Third-Party Lifecycle Management System		**SBI**

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 EOI)	1. Shri Amit Kumar Jain. Designation: Deputy General Manager 2. Shri Vikas Kumar Designation: Asst. General Manager State Bank of India, Vendor Management, Non-IT. Third Party Management Dept. 14th Floor, State Bank Bhawan, Corporate Centre Mumbai Contact Number: 022-22742490 22741458 e-Mail ID: dgm.vmcc@sbi.co.in agm1.vmcc@sbi.co.in
2	Bid Document Availability including changes/amendments, if any to be issued	EOI may be downloaded from Bank's website https://www.sbi.co.in Procurement News and e-Procurement Agency Portal https://etender.sbi/SBI/ from 05.12.2025 to 26.12.2025.
3	Last date for requesting clarification	Up to 14:00 hrs. (time) on 10.12.2025 (date) All communications regarding points / queries requiring clarifications shall be given in writing or by e-mail.
4	Pre - bid Meeting	From 15:00 hrs. (time) to 17:00 hrs. (time) on 15.12.2025 (date) through online meeting.
5	Clarifications to queries raised at pre-bid meetings will be provided by the Bank.	On 20.12.2025 (date)
6	Last date and time for Bid submission	Up to 16:00 (time) on 26.12.2025 (date)
7	Address for submission of Bids	Online through https://etender.sbi/SBI
8	Date and Time of opening of Technical Bids	17:00 hrs. (time) on 26.12.2025 (date) Authorized representatives of Bidders may be present online during the opening of the Technical Bids. However, Technical Bids would be opened even in the absence of any or all Bidders' representatives.

9	Tender Fee	Rs. 25000/- (Rs. Twenty-Five Thousand only) Amount should be deposited in A/c No: 10768099503 IFSC: SBIN0008586 Account Name: MS SBI Central Office, MD A/C, mentioning EOI No. SBI:TPM:CC: EOI:2025-26:01 dt. 05.12.2025. Mode of Transaction- NEFT/ Bank Transfer only. Tender fee will be non-refundable. Proof of tender fee payment to be uploaded along with the technical bid.
10	Contact details of e-Procurement agency appointed for e-procurement	E-Procurement Technologies Ltd A-201/208, Wall Street-II, Opp. Orient Club, Nr. Gujarat College, Ellis Bridge, Ahmedabad – 380 006. **e-mail:** etender.support@sbi.co.in 7859800621, 7859800624, 6352631766, 7859800609, 7990334985, 9510813528, 9081000427

Part-I

Part-II

1. **INVITATION TO BID:**

   i. **State Bank of India** (herein after referred to as **'SBI/the Bank')**, having its Corporate Centre at Mumbai, various other offices (LHOs/ Head Offices /Zonal Offices/Global Link Services, Global IT Centre, foreign offices etc.) of State Bank of India, branches/other offices, Subsidiaries and Joint Ventures available at various locations and managed by the Bank (collectively referred to as **State Bank Group or 'SBG'** hereinafter). This Request for EOI is issued by **the Bank** on behalf of **SBG** for procurement of an integrated software application for end-to-end lifecycle management of outsourcing activities.

   ii. In order to meet the IT requirements, the Bank proposes to invite online EOI from eligible Bidders wishing to be considered for short listing for participating in the bidding process of the proposed procurement.

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

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

   v. The objective of this EOI is to identify eligible Bidders who are interested in providing the required product and services and have suitable capacity, capability and experience.

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

   viii. Interested Bidders are advised to go through the entire EOI before submission of online Bids to avoid any chance of elimination. The criteria and the actual process of evaluation of the responses to this EOI and subsequent selection of the successful Bidder will be entirely at Bank's discretion.

2. BACKGROUND:

With the objective of having one click view of all IT, Non-IT and Non-Banking vendor engagements and to have a single portal for entire third-party life cycle management catering to the requirements of all the departments, to effectively manage existing and emerging risks, procurement of a standalone Software Solution through open market participation is being envisaged.

Brief Introduction of proposed solution scope:

The proposed solution should cover all the following stages/features (not exhaustive indicative only) in built with the following journeys readily available or customizable. The proposed solution can have module workflows clearly demarked as below.

a) **Set Up**- The proposed solution should have three independent modules for catering to – (i) IT related outsourced activities and IT Related Non-outsourced activities, (ii) Outsourcing in Non-IT Banking related activities and (iii) Outsourcing in Non-Banking activities to take care of independent requirement of each outsourcing type.

b) **Pre-Onboarding/Procurement Initiation**: Outsourcing agencies/individuals pre-onboarding processes like provision for upload of minutes of Outsourcing Vetting Committee and compliance to its observations, formation of Bank's internal STPNC committee digitally identified through 'Procurement ID' throughout the system having documents upload facilities (wherever required), allocation of STPNC from Bank's predefined committees pool, capturing proceedings of each STPNCs and finalization of vendor selection etc., Implementation of Generative Artificial Intelligence (GEN AI) for Scanning the market; preparation of RFP including SLA Targets, Key Indicators, Penalty Matrix, Project Milestone; Compliance to Govt. of India /Bank's Procurement guidelines; Responding to Pre-bid Queries and complete end-to-end digital RFP management platform.

c) **On-boarding** : On-boarding process journeys consists of ability to generate auto Financial Sanction documents, PO generations from the system, Legal vetting by the Law Officials, Risk assessments during pre on-boarding process for the outsourcing agency/individual, ability to tag all the individual resources under an agency, provision for interoperability of resources from one agency to another (if required), capturing all the details of Agency/individual resources police verification, Background checks with relevant documents upload features having a centralized pool of categorized document library etc., conducting due diligence on the finalized vendors viz. KYC verification for vendors and beneficial owners, API linkage for verifying details through various monitoring sites viz. NSDL, GSTIN, IBA Caution List, Internal Negative List etc. Module for feeding Sub-

contracting arrangements, due diligence on such arrangements viz. recording prior approvals obtained, upload of executed SLA with the sub-contractors and due diligence documents, evaluation undertaken for suitability of the sub-vendors. Option for upload of the visit reports/ checklist prepared, to be made available.

d) **Post On-Boarding**: SLA Management journey features like digital SLA execution for both onboarding departments and vendors, maintaining Master SLA of an agency, Individual one on one SLA, linking facility of SUB SLAs under a Master SLA, MIS generation using by mentioning SLA ID, system should able to fetch all the resources tagged under the SLA, ability to validate duplicate resources on-boarding with exceptions allowed etc, Ability to input standard Penalty clauses against each SLA in the system, enforces these penalties in various workflows envisaged in the proposed solution or alerts to be generated from the system wherever Penalty clause breached etc. Mechanism for escalation to the mapped Departments such Law, Information Security, Risk etc. be provided, basis various validations/triggers. Different formats applicable to IT, Non-IT and Non-Banking related outsourcing are to be provided in drop-down mode to enable the onboarding depts. to choose suitable format to be used.

e) Proposed system should have its own **Billing module** with provision to incorporate Budgeted amounts, actual consumption amounts as per the SLA's incorporated in the system, which can prepare finalized Bills as per the contracts covering GST/TDS components and its's various components as per the requirement, ability to have aggregation facilities of all the Bills generated from the system like Bank level GST, TDS for a set of outsourcing agencies or entire outsourcing activities etc., ability to integrate with the existing Bank's Billing system by providing all the relevant details for the system and able to ingest reverse feed from the Bank's Billing system and mark closures of the Bills generated from the proposed system. Further, a mechanism for stoppage of bill processing needs to be made available in cases of non- compliance with due diligence measures, risk related compliance etc. A retention sub-module under Billing module needs to be provided that can be utilized to manage, hold and release a part of billed invoices, as per the requirement of onboarding depts.

f) Proposed system must have a **Risk module** which covers all the regulatory requirements of assessing Third party Risk assessments at the time of onboarding and on ongoing basis of vendor and its subcontracting relationships. The third-party risk assessment to include review of vendor's due diligence, verification of financial and operational capabilities, Business continuity/Contingency planning, monitoring of SLA breaches, Reporting of SLA breaches to top management in an automated mode, Penalty and vendor complaints, SLA management, internal review mechanism, Insurance etc. Linkage to OVC module is also to be facilitated. The assessment criteria's (Value statements) to be made flexible and provision to

modify the same with insert/delete option to be made available. Also, Uniform structure for finalization of rating based on the assessment to be made available. Wherever applicable Information security related aspects also need to be validated from the Information Security Department. The risk assessment procedure to be carried out by roles assigned with concerned department, risk department and Information Security department. Data to be fetched from other modules as well to support the risk assessment procedure, viz. Whether SLA is expired? The risk assessment also to be carried out at Exit/Termination stage and basis which vendor to be disabled/debarred on the portal. Dynamic report generation mechanism to be facilitated, projecting the risk associated with the unit/Bank level.

g) **Vendor KYC periodicity** menu to be provided, wherein depending upon the risk category, contract value, no. of contract, no. of resources onboarded, criticality of engagement etc., KYC updation of such vendors and their Beneficial Owners needs to be updated in the application.

h) The proposed system must **adhere to all the Information Security systems mandates** from time to time, cyber risk assessments and follows in accordance with the Information Security policies of the Bank.

i) The proposed system shall **fulfil MIS requirements** like Procurement ID wise, Vendor/Agency ID wise, Individual resources Resource ID wise, PAN/TAN wise aggregations dynamically, using the data/information available in the system, system should be able to generate newer insights covering Risk, Performances of agencies/individuals, Breaches of SLA etc. dynamically. System should categorize the system broadly in pre-on-boarding with Procurement ID, Post on-boarding stage with SLA ID or Vendor ID (Agency ID)/Resource ID, both Procurement ID and SLA ID always be available for each newer procurements of outsourcing activity journey's, in addition search facility available with individual based like search by mobile number, by PAN/TAN number, by Invoice number etc.

j) The proposed system should **be modular in design** (broadly classified as Procurement module (includes goods and services), Vendor/Outsourcing engagement module covering all the sub areas like Billing Module, Risk assessment Module, Penalty management module, performance module) having independent functionalities as well as interoperable functionalities built in. Proposed system should be highly parameterized having flexibility in incorporating futuristic parameters in each of the above modules dynamically without change of code like low code/no code architecture. In summary proposed system should be able to cater the needs of information required from procurement of goods/services inclusive of on-boarding of the services/goods to end of contracts/life of the goods.

k) The proposed system should be on its own **capable of digitally storing information** like various mandatory documents, scanned documents, photographs/images, record GPS coordinates etc., in a secure way such that at all times the data should be always encrypted both at rest and at motion. The system should have across all the modules, maker/checker functionality always available at each journey by default.

l) The proposed system is expected to **have the latest technologies used** like own intelligence to check against various monitoring portals; kind of artificial intelligence models built into the system to provide various analytical reports basis on the information available in the above modules.

m) Further, with a view to the **Information Security compliance** perspective, the proposed solution should provide as under:
- o A module where Information Security Officials can create / assign the Risk Assessment to specific Auditors for independent assessment.
- o An interface wherein, for each assessment, the Team to be mapped for that specific assessment.
- o Facility for uploading Risk Questionnaires in Bulk.
- o Functionality for Assigning weightage at Domain Level, Question Level, Response Level
- o Functionality to alert the auditors if the response to questions by auditee is contradictory in nature.
- o An interface for the Auditee entity to upload evidence.
- o Functionality for marking comments by the Auditor in case the evidence is not appropriate which should be communicated to the Auditee for further compliance
- o The Risk Dashboard should be with multiple use cases: Vendor Wise, Nature of Service Wise, Domain Wise
- o Major areas of concern for a particular Third-Party
- o Major Risk Areas across Third parties etc.
- o Age wise Security Posture of a particular Third-Party
- o A scheduler that indicates when the next review is due for a Third party and alert all stakeholders.
- o A downloadable report which indicates the complete list of observations for each third Party.
- o A report to download the Third-Party Master along with the date of the last Security Review.
- o The application should facilitate Assessment in multiple stages such as Onboarding, Continuous Assessment and Periodic Assessment.

o Threat Intelligence feed about the Third-Party to be provided.

n) Security Measures Expected in the Application / Third-Party includes but not limited to the following: -
   o The Application should ensure Confidentiality (both in transit and at Rest), and Integrity
   o Content filtering to be ensured for any file uploaded by the Third Party as evidence o The application should support integration with Security Solution such as SIEM, DAM, PIMS, ITAM, DLP, IRM, O365, AD
   o The Application should support integration with the Bank's EIS (wherein APIs would be Channel and Payload encrypted as well as Digitally Signed)
   o The Application should support multiple data formats for API integration
   o The Application should support Maker-Checker functionality at all modules (which should be configurable as per the requirement)
   o CERT-In empaneled auditors report on the complete Application covering Gray Box Appsec, Source Code Review, API Review (the scope of which should be minimum OWASP Top 10 and SANS 25), Source Code Review etc.
   o Compliance to the controls as laid down in Supply Chain Cyber Risk Assessment SOP of the Bank.
   o Any Security vulnerability reported by the Bank at any point in time, should be fixed in a time bound manner
   o Security Patches to be provided by the OEM periodically or immediately as necessitated (whichever is earlier)
   o Any Common Vulnerabilities and Exposures (CVEs) in the application to be reported to the Bank, which would be reviewed by the Bank and decide the subsequent course of action.
   o Any Security Incident at the OEM environment should be reported to the Bank immediately.
   o This requirement can be modified or updated subject to Bank's security requirement.
o) Data migration from Bank's existing system should be seamless. Solution provider should have such tools that are time efficient.
p) The Proposed system should be interoperable i.e. it can be integrated with future systems (if required). It should be capable of using AI/ML for predictive risk, fraud detection and SLA optimization.
q) The proposed system must be scalable i.e. in future if 10,000+ vendors need to be added, its performance should not downgrade.
r) The solution provider should be able to update the system as per the prevailing guidelines of regulators i.e. RBI, SEBI, etc. and various relevant acts such as Digital Personal Data Protection Act 2023.
s) Bank's Data Protection Policy to be strictly adhered to and no data should go out of the Bank domain.

t) The solution provider needs to have a Cyber Insurance Policy covering entire gamut of the proposed Third-Party Lifecycle Management System, with proof shared annually with the Bank.

u) Annual third-party security audits of the application must be arranged by the solution provider and reports to be shared with the Bank.

v) A mandatory training for Bank staff/ maintenance team plus refresher sessions every year to be arranged by the developer.

w) Documentation of the proposed application and FAQs to reduce dependency on the developer for maintenance team.

x) Dedicated support team along with escalation matrix needs to be provided for initial 2-3 years.

y) The developer needs to propose one improvement/ innovation clause in its annual improvement plan.

z) The solution provider to ensure minimum 99.9% uptime of the solution.

The proposed solution is expected to provide the following benefits:

i. Complete automation of end-to-end process i.e. onboarding of vendors, SLA library, maintenance of records, realistic monitoring of activities.

ii. Automatic flow of data from onboarding to later stages on completion of various tasks.

iii. Objective risk assessment based on specific value statements with automated scoring and real time monitoring at the time of prior to onboarding, post onboarding, periodic reviews, termination and exit.

iv. Minimizing manual interventions through intelligent workflows and system driven validations.

v. Onboarding and management of vendors engaged in IT & Non-IT Banking related activities as well as Non - Banking activities covered under RBI Outsourcing Policy.

vi. Integration of flow of information from various monitoring sites viz. Internal Negative List (INL) Portal, IBA Caution Listing, NSDL, GSTIN Portals etc.

vii. Integration of the Portal with Vendor Payment System (VPS) to ensure effective monitoring of vendors' bill payments.

viii. Facilitating decision-making through comprehensive dashboards and dynamic MIS reporting.

ix. Seamless migration of data from existing applications.

x. Identification and automatic escalation of SLA breaches, compliance failures, Penalty for the same.

xi. Integration of the Portal with Bank's Outsourcing Audit/ IS Audit Portal for smooth flow of data and flagging of irregularities by Audit Dept.

3. **DISCLAIMER:**

i. The information contained in this EOI, 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 EOI.

ii. This EOI is not an offer by SBI, but an invitation to receive responses from the eligible Bidders.

iii. The purpose of this EOI is to provide the Bidder(s) with information to assist preparation of their Bid proposals. This EOI 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 EOI 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 EOI.

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 EOI or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the EOI and any assessment, assumption, statement or information contained therein or deemed to form or arising in any way for participation in this EOI.

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 EOI.

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

vii. The issue of this EOI does not imply that the Bank is bound to select a Bidder or subsequently to award the contract to the shortlisted 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.

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 EOI.

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

5. **ELIGIBILITY AND TECHNICAL CRITERIA/SCOPE OF WORK**:

   i. Bid is open to all Bidders who meet the eligibility and technical criteria/scope of work as given in **Appendix-B & Appendix-C** of this EOI. The Bidder has to submit the documents substantiating eligibility criteria as mentioned in this EOI 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 EOI. Bid submitted with options of multiple OEMs shall also be considered Bid submitted on behalf of multiple OEMs.

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

6. **COST OF BID DOCUMENT:**

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

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

   i. Bidder requiring any clarification on EOI may notify the Bank in writing strictly as per the format given in **Appendix-E** at the address/by e-mail within the date/time

mentioned in the Schedule of Events.

ii. All queries to be raised in the pre-bid meeting will relate to the EOI alone and no queries related to detailed analysis of scope of work, payment terms and mode of selection will be entertained. These issues will be amply clarified at the RFP stage.

iii. 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 EOI.

iv. 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.

v. The Bank reserves the right to amend, rescind or reissue the EOI, 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 EOI, 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.

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

8. **CONTENTS OF EOI DOCUMENT:**

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

ii. Failure to furnish all information required in this EOI or submission of Bid not responsive to this EOI 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 EOI 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 EOI will become the property of the Bank and will not be returned. Incomplete information in Bid document may lead to non-consideration of the proposal.

9. **BID PREPARATION AND SUBMISSION:**

i. The Bid is to be submitted on portal of e-Procurement agency for EOI of procurement of a Third-Party Lifecycle Management software application for end-to-end lifecycle management of outsourcing activities in response to the EOI No. SBI:TPM:CC: EOI:01 dated 05.12.2025. Documents mentioned below are to be uploaded on portal of e-Procurement agency with digital signature of authorised signatory:

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

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

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

(d) Specific response with supporting documents in respect of Eligibility Criteria as mentioned in **Appendix-B** and technical criteria/scope of work 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, copy of registration certificate issued by competent authority as mentioned in **Sl No 2 of Eligibility Criteria** under **Appendix-B**.

ii. **Bidders may please note:**

(a) While submitting the Technical Bid, literature on the proposed solution/services should be segregated and kept together in one section.

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

(c) 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 EOI. DSC should be in the name of the authorized signatory. It should be in corporate capacity (that is in Bidder capacity).

(d) 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.

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

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

(g) 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.

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

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

(j) 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 representatives to Bid and make commitments on behalf of the Bidder is to be attached.

(k) 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.

(l) 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.

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

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.

11. MODIFICATION AND WITHDRAWAL OF BIDS:

i. The Bidder may modify or withdraw its Bid after the Bid's submission, provided that 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.

12. **BIDDING PROCESS/OPENING OF TECHNICAL BIDS:**

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

iii. 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.

iv. After examining the EOI, some or all of the Bidders may be asked to make presentation of the solution and demonstrate proof of concept (POC). The Bidder shall bear all costs associated with submission of EOI, presentation/POC desired by the Bank. The Bank shall not be responsible or liable for any cost thereof, regardless of the conduct or outcome of the process.

v. SBI may shortlist the Bidders who fulfill the eligibility and technical criteria specified in this EOI, have solution/services as per the requirement of the Bank and are agreeing to abide by the terms and conditions of the Bank. Bank's judgment in this regard will be final.

vi. Bank may issue a Request for Proposal (RFP) to shortlisted Bidder for next process of procurement. However, short listing of Bidders shall not be treated as a contract for the proposed work. Guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order) and any revision, clarification and amendment thereto will also be applicable to the RFP.

vii. Participating bidders need to sign and submit Pre-Contract Integrity Pact, based on the estimated value of procurement at the time of submitting bids during RFP process as per Appendix –G.

viii. Nothing contained in this EOI shall impair the Bank's Right to issue 'Open RFP' on the proposed solution/services.

ix. Bidders will be advised about shortlisting of their EOIs or otherwise. However, Bidders will not be provided with information about comparative position of their EOIs with that of others.

13. **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 without prejudice to any other right or remedy that may be available to the Bank under the EOI and/ or the subsequent RFP 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 EOI.

iii. For the purposes of this EOI, 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.

14. **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 EOI 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 declarations or providing false information for participation in a EOI 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 Bidder is found lacking in performance, in case of less frequent and less serious misdemeanors, the Bidders may be put on a holiday listing (temporary debarment) for a period upto 12 (twelve) months. When a Bidder 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 Bidder 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.).

- Bidders undergoing process for removal from empanelment/participation in procurement process or banning/debarment may also be put on a holiday listing during such proceedings.

(b) Debarment from participation including removal from empaneled list

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

- Without prejudice to the rights of the Bank under Clause 14(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.

- The Bidder 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 Bidder 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 Bidder 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 Bidder (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.

15. GOVERNING LANGUAGE:

The governing language shall be English.

16. 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.

17. 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.

18. **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.

19. **NOTICES:**

Any notice given by one party to the other pursuant to this EOI shall be sent to other party in writing 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.

20. **OTHER TERMS & CONDITIONS**

i. Lodgement of an EOI is evidence of a Bidder's consent to comply with the terms and condition of Request for EOI process and subsequent bidding process. If a Bidder fails to comply with any of the terms, its EOI may be summarily rejected.

ii. Willful misrepresentation of any fact within the Bid will lead to the disqualification of the Bidder 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.

iii. Bidders must advise the Bank immediately in writing of any material change to the information contained in the EOI application, including any substantial change in their ownership or their financial or technical capacity. Copies of relevant documents must be submitted with their advices. For shortlisted Bidders, this requirement applies until a contract is awarded as a result of subsequent bidding process.

iv. Shortlisted Bidders must not advertise or publish the same in any form without the prior written consent of SBI.

v. Brief overview of the proposed procurement/scope of work given in this document may be further elaborated, viz., more details may be included in the Request for Proposal (RFP) document to be issued as a result of evaluation process of EOIs.

vi. The Bank reserves the right to formulate any terms & conditions while framing the RFP, even if these are in variance with the terms provided in this EOI. Further, the Bidders shall have no claim in this regard.

vii. The Bank shall have the right to cancel the EOI process itself at any time, without thereby incurring any liabilities to the affected Bidders. Reasons for cancellation, as determined by the Bank in its sole discretion include but are not limited to, the following:
   a. Services contemplated are no longer required.
   b. Scope of work not adequately or clearly defined due to unforeseen circumstance and/or factors and/or new developments.
   c. The project is not in the best interest of the Bank.
   d. Any other reason.

PART-II

BID FORM (TECHNICAL BID)

[On Bidder's letter head]

Date: _____

To:

The Deputy General Manager

State Bank of India

Vendor Management, Non-IT

Third Party Management Department

14th Floor, State Bank Bhawan

Corporate Centre,

Nariman Point, Mumbai

Dear Sir,

Ref: EOI No. SBI:TPM:CC: EOI:2025-26:01 dated 05.12.2025

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

We have examined the above EOI, the receipt of which is hereby duly acknowledged and subsequent pre-bid clarifications/ modifications / revisions, if any, furnished by the Bank. We submit our bid and shall abide by the terms and conditions spelt out in the EOI.

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 EOI.

- We have not induced or attempted to induce any other Bidder to submit or not to submit a Bid for restricting competition.

ii. We undertake that, in competing for the above EOI, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".

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

iv. We undertake that we will not resort to canvassing with any official of the Bank, connected directly or indirectly with the EOI 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 this EOI. 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 EOI or any subsequent bidding process 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 EOI, read with its amendments/clarifications provided by the Bank.

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

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

ix. We hereby certify that on the date of submission of Bid for this EOI, 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.

x. 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.

xi. 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 and amendment/ revision 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. We certify that we and our OEM fulfil all the requirements in this regard and are eligible to participate in this EOI.

xii. We further declare as mentioned below:
  - That, the solution/product offered would be compatible with all the guidelines issued by regulatory/ government bodies from time to time.

- That, we have a stable and scalable prepaid solution with access to source code, so that any changes required by the Bank can be carried out expressly.
- That, if offered in public cloud infrastructure, all hardware and software infrastructure for the proposed solution will be deployed in India with servers / portal/ applications uptime not less than 99.999% of servers / portal/ applications. We confirm that no data of the Bank will go out of India through any medium.
- That, we certify and agree that all data generated as part of this program belongs to State Bank of India and is our first party asset. The bidder cannot stake claim or monetize this consumer data along with the transaction behavior from third parties, without the explicit written approval from the Bank.
- That, the solution offered is owned by us or our OEM and we have its IP rights.
- That, we do not have any security incident/vulnerability or information security incident assigned to our hosted or deployed system in last 3 years of operation.
- That, the solution supports end-to- end data encryption at all layers including data at rest and data in motion, with strong encryption algorithm.

xiii. We hereby undertake and agree to abide by all the terms and conditions stipulated by the Bank in the EOI document.

Dated this .... day of 202

_____
(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/ revision thereto.		Bidder should specifically certify in **Appendix A** in this regard and provide copy of the registration certificate issued by competent authority wherever applicable.
3.	The Bidder must have an average turnover of a minimum of Rs. 200 crores crore during last 03 (three) financial year(s) i.e. FY 2022-23, FY 2023-24 and FY 2024-25.		Copy of the audited financial statement for required financial years. (Certificate from statutory auditor for preceding/current year may also be submitted.)
4.	The Bidder should be profitable organization on the basis of profit before tax (PBT) for at least 02 (two) out of last 03 (three) financial years mentioned in para 2 above.		Copy of the audited financial statement along with profit and loss statement for corresponding years and Certificate of the statutory auditor.
5	The bidder should have experience of minimum 03 BFSI clients during the last 05 years in providing the required products/services/solution.		Copy of the order and / or Certificate of completion of the work. The Bidder should also furnish user acceptance report.

6.	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 03 client references are required)		Bidder should specifically confirm on their letter head in this regard as per **Appendix-F**
7.	Certification Requirements (ISO27001, ITIL, COMP, COMIT, ISO37500 (Preferable)		Copy of the Valid Certificate(s) to be provided.
8.	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 EOI 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. However, in case there is no such past/ present litigations, disputes, as sought above, the Bidder may provide self-certificate on Company's letter head that "We hereby certify that as on the date of submission of Bid for this EOI, we do not have any past / present litigation which adversely affects

			our participation or ability to perform our obligations under this EOI."
9.	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 EOI 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.
10.	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.
11.	Bidder solution if offered in Public cloud should have both primary Data Center and DR center with full back up arrangement in different geographical location of India. The facilities should be ISO 27001 certified and audited.		Copies of the latest valid certificates to this affect should be submitted by the bidder.
12.	The solution/product offered should be compatible with all the guidelines issued by regulatory/ government bodies from time to time.		Declaration to this effect must be submitted by the Bidder in the company letterhead vide Para No. xii of Appendix –A.
13.	Bidder or its OEM should have a stable and scalable prepaid solution with access to source code, so that any changes required by the Bank can be carried out expressly.		Declaration to this effect must be submitted by the Bidder in the company letterhead vide Para No. xii of Appendix –A.

14.	If offered in public cloud infrastructure, all hardware and software infrastructure for the proposed solution must be deployed in India with servers / portal/ applications uptime not less than 99.999% of servers / portal/ applications. Bidder to confirm that no data of the Bank is going out of India through any medium.		Declaration to this effect must be submitted by the Bidder in the company letterhead vide Para No. xii of Appendix –A.
15.	Bidder to certify and agree that all data generated as part of this program belongs to State Bank of India and is our first party asset. The bidder cannot stake claim or monetize this consumer data along with the transaction behavior from third parties, without the explicit written approval from the Bank		Declaration to this effect must be submitted by the Bidder in the company letterhead vide Para No. xii of Appendix –A.
16.	The solution offered must be owned by the Bidder or its OEM and must have its IP rights.		Declaration to this effect must be submitted by the Bidder in the company letterhead vide Para No. xii of Appendix –A.
17.	The bidder shouldn't have any security incident/vulnerability or information security incident assigned to their hosted or deployed system in last 3 years of operation.		Declaration to this effect must be submitted by the Bidder in the company letterhead vide Para No. xii of Appendix –A.
18.	The solution should support end-to- end data encryption at all layers including data at rest and data in motion. with strong encryption algorithm.		Declaration to this effect must be submitted by the Bidder in the company letterhead vide Para No. xii of Appendix –A.
19.	Bidder should also have internal control and audit measures in place. Bidder will provide their Internal Audit certificates by a Cert-in empaneled vendor for the preceding financial year from the date of EOI.		Declaration to this effect must be submitted by the Bidder in the company letterhead vide Para No. xii of Appendix –A.

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

Eligibility criteria mentioned at Sl. No 3 to 6 in table above are relaxed for Startups subject to their meeting of quality and technical specifications. Bidder to note the followings:

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

ii. Bidder who solely on its own, fulfils each eligibility criteria condition as per the EOI terms and conditions and who are having Start-up company status, can claim exemption for eligibility criteria mentioned at Sl No 3 to 6 in table above.

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

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

TECHNICAL CRITERIA/SCOPE OF WORK

A. Functional specifications:

These specifications outline what the software must do across the entire third-party lifecycle processes:

❖ **Procurement & Vendor Selection**

- o Support for multi-category procurement (IT, Non-IT & Non-Banking)
- o Configurable vendor evaluation templates
- o Integration with e-Tendering platforms
- o Automated scoring and ranking of vendor bids
- o Auto-ranking of bids based on technical and financial criteria
- o Audit trail for bid evaluation and selection decisions.

❖ **Vendor Onboarding & Compliance**

- o Digital onboarding workflows with document uploads
- o Document checklist (PAN, GST, incorporation, bank details, etc.)
- o Police verification and background check integration
- o KYC/AML compliance checks
- o Geo-tagging and jurisdictional compliance mapping
- o Document checklist (PAN, GST, incorporation, bank details, etc.)
- o Ensure compliance with relevant regulations and policies

❖ **Common Communication and Collaboration**

- o Provide platforms for communication between internal teams and external vendors, fostering collaboration and knowledge sharing

❖ **SLA Preparation & Management**

- o SLA template builder with clause-level customization
- o Approval workflows with version control
- o SLA negotiation and approval workflows
- o SLA breach tracking and penalty automation
- o Escalation matrix and breach notification system
- o SLA renewal and amendment tracking
- o Alerts and escalations for SLA violations

❖ **Billing generation/payments Management**

- o Tagging of Bills with SLA (SLA IDs)
- o Raise of Bills and payment workflows
- o Holding of partial/full amount of Bills raised.
- o Maintaining TAT of Bills as per SLA, alerts

❖ **Vendor Performance Management**

- o KPI dashboards for vendor resources

- Role-based performance tracking (e.g., manpower, delivery)
- Feedback loops and periodic review mechanisms
- Integration with biometric or attendance systems (optional)

❖ **Risk Assessment & Regulatory Adherence**

- Risk profiling based on vendor type, geography, and service category
- Risk scoring engine with mitigation recommendations
- Compliance checklist for local/state/national regulations
- Automated alerts for non-compliance or high-risk vendors
- Integration with audit and legal systems

❖ **Resource Management**

- Resource onboarding/offboarding workflows
- Background verification status tracking
- Attendance and biometric integration (optional)
- Performance alerts and underperformance flags
- Role-based access provisioning and revocation

❖ **Contract Lifecycle Management**

- Clause-level contract creation and approval
- Renewal reminders and auto-renewal options
- Termination workflows with exit checklists
- Archival and retention policy enforcement
- Contract repository with search and tagging

❖ **Security & Access Control**

- Role-based access control (RBAC)
- Multi-factor authentication (MFA)
- Data encryption at rest and in transit
- Audit logs for all user actions
- GDPR and ISO 27001 compliance readiness

❖ **Offboarding**

- Formal termination or renewal of the third-party relationship
- Ensure smooth transition and minimal disruption.

B. Technical Evaluation Criteria:

Bidder to give in their response the codes, as given below in the following Tables (i.e., B1. Mandatory Functionalities and B2. Preferred functionalities. Detailed responses may be provided in table B3- Presentations & Site visits etc. describing how their solution will meet the required parameters and provide details thereof in their EOI Proposal.

Requirements are classified into the following categories:

SYMBOL	CATEGORY
M	Mandatory, application must provide the functionality out-of-box or customize them with no extra cost.
P	Preferable, prefer to have features of the application

Status (Codes)	Description
A	Available
C	Customizable
N	Not feasible

B1: Mandatory Functionalities:

Evaluation Category	Criteria	Category	Compliance Status (A/C/N)
Functional Coverage	Mature Vendor Management Solution in enterprise use	M	
	Data Ingestion Capability (Handles ≥ 20M/ day and 10 B records)	M	
	On-Premises Deployment	M	
Technology Stack & Architecture	Cloud-native (preferably Bank's private cloud- VMWARE) , scalable, modular (preferably microservices); support for APIs and containerization	M	
Integration Capability	Proven integration with ERP (SAP/Oracle/Dynamics), HRMS, e-Tendering, compliance tools; provide architecture diagrams	M	
Security & Compliance	ISO 27001/37500, GDPR, SOC 2 compliance; data encryption, RBAC, audit logs	M	
Customization & Configurability	Workflow builder, form designer, rule engine; no hardcoded logic, preferable low code no code setups	M	
Support & Maintenance	24x7 support, ticketing system, escalation matrix; SLA adherence reports	M	

Evaluation Category	Criteria	Category	Compliance Status (A/C/N)
Domain Expertise	Minimum 5 similar implementations in third-party lifecycle management for the last 5 years out of which at least 2 implementations should be from BFSI sector; case studies required.	M	
Financial Strength	Bidder Net Worth, Turnover Financial Soundness of the Bidder	M	
Integration of flow of information from various monitoring sites	For due diligence on vendors, flow of information from sites like Bank's Internal Negative List (INL) Portal, IBA Caution Listing, NSDL, GSTIN Portals etc.	M	
To ensure effective monitoring of vendors' bill payments.	Integration of the Portal with Bank's Vendor Payment System (VPS). The System should have also its own Billing module.	M	
Facilitating decision-making and data analysis	Comprehensive dashboards and dynamic MIS reporting.	M	
Seamless migration of data from existing applications	Migration of data from Bank's existing owned applications i.e. OLMS/ PLMS /CBPS/ PRMS / TPRM	M	
Tech Functionality	Utility for identification and auto escalation of SLA breaches, compliance failures, Penalty for the same, penalty recovery data etc.	M	
Smooth flow of data related to Audit irregularities & compliances	Integration of the Portal with Bank's IT/ Non-IT/ IS Audit Portals	M	
Complete automation of end-to-end process	From onboarding of vendors, SLA library, maintenance of records, realistic monitoring of activities etc.	M	
Data flow	Automatic flow of data from onboarding to later stages on completion of various tasks.	M	
Risk management	Functionality for objective risk assessment based on specific value statements and automated scoring and real time monitoring at various stages.	M	
Limited manual interventions	Incorporating intelligent workflows and system driven validations.	M	

Evaluation Category	Criteria	Category	Compliance Status (A/C/N)
Automated Notifications and Alerts	System driven automated notifications and alerts at defined periodicity	M	
Automated Procurement processes	Module for initiating and finalization of the procurement process. Functionality for allocation of TPNC and capturing the details.	M	
Management of vendor employee's data	Module for on boarding/ off- boarding the vendor resources and the process workflow.	M	
Periodic Review	Module for periodic Review of Vendor Performance	M	
Vendor blacklisting	Module for vendor blacklisting/ caution listing and API integration of INL Portal/ IBA Caution List.	M	
Complaints management	Module for recording complaints against vendors, resolutions and timelines.	M	
SLA Management	Automated SLA creation and functionality for digital signature	M	
	Auto-allocation of SLAs to Law section, in case of modifications, additions, deletions etc.	M	
Compliances related to Sub-contracting	Module for sub-contracting- functionality for according prior approval, technical evaluation, SLA recording etc.	M	
Security & Access Control Management	User records, event records, Role Based Access Control etc.	M	

B2. **Preferred functionalities:**

Evaluation Category	Criteria	Category	Status (A/C/N)
Client References & Case Studies	At least 2 references with similar scale and complexity; contact details required	P	
Market Leadership & Recognition	Recognition by Gartner or Forrester	P	
Solution Features	Must meet all functional specifications listed in Point No. **(A)** **Functional specifications** above; partial coverage gets proportionate marks	P	

Early Warning Systems	To Predict potential vendor failures or SLA breaches through anomaly detection and trend analysis.	P	
Ongoing Monitoring & Risk Assessment	Real-time tracking of third-party risk indicators using AI models trained on financials, service data, customer feedback, and external alerts.	P	
AI-powered Risk Profiling during Due Diligence	Automated background checks using NLP (Natural language Processing) to extract insights from external sources (financials, media, legal, regulatory watchlists etc.)	P	
Experience & Track Record	No. of Large VMS Implementations in 5 Years	P	
	Large Public/ Private Sector BFSI Client	P	
Training & Documentation	User manuals, onboarding guides, video tutorials, admin training	P	
Cost Effectiveness	TCO analysis, licensing model (subscription/perpetual), scalability of pricing	P	

B 3: Presentation and Alignment with the requirement:

Sl. No.	Parameters	Compliance Status

1.	Degree of alignment of the solution being proposed with the requirements of the Bank. This would be ascertained through presentations / demonstrations / documents / visits to the customer location, management centers of the bidders
	    A. Does the bidder display clear understanding in fulfilling the bank's requirements mentioned in RFP?
	    B. Does the bidder demonstrate the ability to deliver on all mandatory requirements beyond any doubt?
	    C. Does the bidder have capabilities to support the implementation and have the implementation road-map available?
	    D. Ability to provide innovative ideas and card variants to capture new business or meet competition.	

Note:

- Any wrong reporting in the above column which subsequently found to be false shall render the applicant liable to be blacklisted for future participation in the RFPs/Tenders of the Bank and EMD will be forfeited.
- Supporting documents will be verified only if the Bidder satisfies the minimum criteria laid above.
- Eligibility of the Bidder will be based on totality and if all conditions satisfy each Required Functionalities/ Features mentioned above.

Technical and functional specifications mentioned above are complementary to Broad scope of work in Appendix-E. Final implementation in the Bank will cover Technical and functional specifications, Broad Scope of Work in entirety.

Scope of Work

Table of Contents

1. INTRODUCTION

1.1 **Purpose**

This document provides the requirements and functionalities for the Third-Party Lifecycle Management System designed for SBI to manage IT, Non-IT and Non-Banking activities outsourced to third-party agencies and risk associated with it, in compliance with RBI guidelines. The system will automate the complete vendor lifecycle, ensuring transparency, compliance, and efficient decision-making.

Current Position

Presently Bank utilizes internally developed 06 platforms for managing outsourcing vendors in IT and Non-IT activities. No portal/ application is utilized for managing Non-Banking vendors. While Outsourcing Lifecycle Management System (OLMS) application is used for both IT and Non-IT activities, IT Partner Relationships Dept. extensively utilizes its Procurement Lifecycle Management System (PLMS), SLA Management System (SLAMS), Partner Resource Management System (PRMS) and Centralized Bill Processing System (CBPS) applications for managing IT outsourcing activities. For managing operational risk-related aspects, one more portal Third-Party Risk Management (TPRM) Portal is in use.

It has been envisioned to procure an integrated Outsourcing Management System which will encompass all the processes undertaken using existing portals and sunset the existing portals after migrating all the data to the new platform.

Bank currently manages approximately 5000 vendors, 1250 users through the portals. Data related to vendors viz. agency details, Beneficial Owners' details, SLA scanned documents, monitoring documents viz. BCP, Annual/ Semi Annual Review data, Audit records etc. and user details are required to be migrated to new platform. With the inclusion of non- Banking vendors, the new portal is expected to be capable to manage 10000 vendors, 5000 users and more than 100 types of activities.

1.2 Objective

• Automate vendor onboarding, sub-contractor management, SLA tracking, Third Party Risk Assessment and audit processes.

• Ensures compliance with regulatory guidelines (e.g., RBI).

• Facilitates decision-making through comprehensive dashboards and dynamic MIS reporting.

• Seamless migration from Existing applications (PLMS/ CBPS/ PRMS/ OLMS).

1.3 Scope

The proposed solution can have module workflows clearly demarcated as below.

a) **Set Up**- The proposed solution should have three independent modules for catering to – (i) IT related outsourced activities and IT Related Non-outsourced activities (ii) Outsourcing in Non-IT Banking related activities and (iii) Outsourcing in Non-Banking activities to take care of independent requirement of each outsourcing type.

b) **Pre-Onboarding/Procurement Initiation**: Outsourcing agencies/individuals pre-onboarding processes like provision for upload of minutes of Outsourcing Vetting Committee and compliance to its observations, formation of Bank's internal STPNC committee digitally identified through 'Procurement ID' throughout the system having documents upload facilities (wherever required), allocation of STPNC from Bank's predefined committees pool, capturing proceedings of each STPNCs and finalization of vendor selection etc. Implementation of Generative Artificial Intelligence (GEN AI) for Scanning the market; preparation of RFP including SLA Targets, Key Indicators, Penalty Matrix, Project Milestone; Compliance to Govt. of India /Bank's Procurement guidelines; Responding to Pre-bid Queries and complete end-to-end digital RFP management platform.

c) **On-boarding** : On-boarding process journeys consists of ability to generate auto Financial Sanction documents, PO generations from the system, Legal vetting by the Law Officials, Risk assessments during pre on-boarding process for the outsourcing agency/individual, ability to tag all the individual resources under an agency, provision for interoperability of resources from one agency to another (if required), capturing all the details of Agency/individual resources police verification, Background checks with relevant documents upload features having a centralized pool of categorized document library etc., conducting due diligence on the finalized vendors viz. KYC verification for vendors and beneficial owners, API linkage for verifying details through various monitoring sites viz. NSDL, GSTIN, IBA Caution List, Internal Negative List etc. Module for feeding Sub-contracting arrangements, due diligence on such arrangements viz. recording prior approvals obtained, upload of executed SLA with the sub-contractors and due diligence documents, evaluation undertaken for suitability of the sub-vendors. Option for upload of the visit reports/ checklist prepared, to be made available.

d) **Post On-Boarding**: SLA Management journey features like digital SLA execution for both onboarding departments and vendors, maintaining Master SLA of an agency, Individual one on one SLA, linking facility of SUB SLAs under a Master SLA, MIS generation using by mentioning SLA ID, system should able to fetch all the resources tagged under the SLA, ability to validate duplicate resources on-boarding with exceptions allowed etc., Ability to input standard Penalty clauses

against each SLA in the system, enforces these penalties in various workflows envisaged in the proposed solution or alerts to be generated from the system wherever Penalty clause breached etc. Mechanism for escalation to the mapped Departments such Law, Information Security, Risk etc. be provided, basis various validations/triggers. Different formats applicable to IT, Non-IT and Non-Banking related outsourcing are to be provided in drop-down mode to enable the onboarding depts. to choose suitable format to be used.

e) Proposed system should have its own **Billing module** with provision to incorporate Budgeted amounts, actual consumption amounts as per the SLA's incorporated in the system, which can prepare finalized Bills as per the contracts covering GST/TDS components and its's various components as per the requirement, ability to have aggregation facilities of all the Bills generated from the system like Bank level GST, TDS for a set of outsourcing agencies or entire outsourcing activities etc., ability to integrate with the existing Bank's Billing system by providing all the relevant details for the system and able to ingest reverse feed from the Bank's Billing system and mark closures of the Bills generated from the proposed system. Further, a mechanism for stoppage of bill processing needs to be made available in cases of non- compliance with due diligence measures, risk related compliance etc. A Bill Retention sub-module under Billing module needs to be provided that can be utilized to manage, hold and release a part of billed invoices, as per the requirement of onboarding depts.

f) Proposed system must have a **Risk module** which covers all the regulatory requirements of assessing Third party Risk assessments at the time of onboarding and on ongoing basis of vendor and its subcontracting relationships. The third-party risk assessment to include review of vendor's due diligence, verification of financial and operational capabilities, Business continuity/Contingency planning, monitoring of SLA breaches, Reporting of SLA breaches to top management in an automated mode, Penalty and vendor complaints, SLA management, internal review mechanism, Insurance etc. Linkage to OVC module is also to be facilitated. The assessment criteria's (Value statements) to be made flexible and provision to modify the same with insert/delete option to be made available. Also, Uniform structure for finalization of rating based on the assessment to be made available. Wherever applicable Information security related aspects also need to be validated from the Information Security Department. The risk assessment procedure to be carried out by roles assigned with concerned department, risk department and Information Security department. Data to be fetched from other modules as well to support the risk assessment procedure, viz. Whether SLA is expired? The risk assessment also to be carried out at Exit/Termination stage and basis which vendor to be disabled/debarred on the portal. Dynamic report generation mechanism to be facilitated, projecting the risk associated with the unit/Bank level.

g) A budget module needs to be provided to take care of the budgeting requirements.

h) Vendor KYC periodicity menu to be provided, wherein depending upon the risk category, contract value, no. of contract, no. of resources onboarded, criticality of engagement etc., periodic KYC updation of such vendors and their Beneficial Owners needs to be updated in the application.

i) The proposed system must **adhere to all the Information Security systems mandates** from time to time, cyber risk assessments and follows in accordance with the Information Security policies of the Bank.

j) The proposed system shall **fulfil MIS requirements** like Procurement ID wise, Vendor/Agency ID wise, Individual resources Resource ID wise, PAN/TAN wise aggregations dynamically, using the data/information available in the system, system should be able to generate newer insights covering Risk, Performances of agencies/individuals, Breaches of SLA etc. dynamically. System should categorize the system broadly in pre-on-boarding with Procurement ID, Post on-boarding stage with SLA ID or Vendor ID (Agency ID)/Resource ID, both Procurement ID and SLA ID always be available for each newer procurements of outsourcing activity journey's, in addition search facility available with individual based like search by mobile number, by PAN/TAN number, by Invoice number etc.

k) The proposed system should **be modular in design** (broadly classified as Procurement module (includes goods and services), Vendor/Outsourcing engagement module covering all the sub areas like Billing Module, Risk assessment Module, Penalty management module, performance module) having independent functionalities as well as interoperable functionalities built in. Proposed system should be highly parameterized having flexibility in incorporating futuristic parameters in each of the above modules dynamically without change of code like low code/no code architecture. In summary proposed system should be able to cater the needs of information required from procurement of goods/services inclusive of on-boarding of the services/goods to end of contracts/life of the goods.

l) The proposed system should be on its own **capable of digitally storing information** like various mandatory documents, scanned documents, photographs/images, record GPS coordinates etc., in a secure way such that at all times the data should be always encrypted both at rest and at motion. The system should have across all the modules, maker/checker functionality always available at each journey by default.

m) The proposed system is expected to **have the latest technologies used** like own intelligence to check against various monitoring portals; kind of artificial intelligence models built into the system to provide various analytical reports basis on the information available in the above modules.

n) Further, with a view to the **Information Security compliance** perspective, the proposed solution should provide as under:

   o A module where Information Security Officials can create / assign the Risk Assessment to specific Auditors for independent assessment.
   o An interface wherein, for each assessment, the Team to be mapped for that specific assessment.
   o Facility for uploading Risk Questionnaires in Bulk.
   o Functionality for Assigning weightage at Domain Level, Question Level, Response Level
   o Functionality to alert the auditors if the response to questions by auditee is contradictory in nature.
   o An interface for the Auditee entity to upload evidence.
   o Functionality for marking comments by the Auditor in case the evidence is not appropriate which should be communicated to the Auditee for further compliance
   o The Risk Dashboard should be with multiple use cases: Vendor Wise, Nature of Service Wise, Domain Wise
   o Major areas of concern for a particular Third-Party
   o Major Risk Areas across Third parties etc.
   o Age wise Security Posture of a particular Third-Party
   o A scheduler that indicates when the next review is due for a Third party and alert all stakeholders.
   o A downloadable report which indicates the complete list of observations for each third Party.
   o A report to download the Third-Party Master along with the date of the last Security Review.
   o The application should facilitate Assessment in multiple stages such as Onboarding, Continuous Assessment and Periodic Assessment.
   o Threat Intelligence feed about the Third-Party to be provided.

o) Security Measures Expected in the Application / Third-Party includes but not limited to the following: -

   o The Application should ensure Confidentiality (both in transit and at Rest), and Integrity
   o Content filtering to be ensured for any file uploaded by the Third Party as evidence o The application should support integration with Security

Solution such as SIEM, DAM, PIMS, ITAM, DLP, IRM, O365, AD

- o The Application should support integration with the Bank's EIS (wherein APIs would be Channel and Payload encrypted as well as Digitally Signed)
- o The Application should support multiple data formats for API integration
- o The Application should support Maker-Checker functionality at all modules (which should be configurable as per the requirement)
- o CERT-In empaneled auditors report on the complete Application covering Gray Box Appsec, Source Code Review, API Review (the scope of which should be minimum OWASP Top 10 and SANS 25), Source Code Review etc.
- o Compliance to the controls as laid down in Supply Chain Cyber Risk Assessment SOP of the Bank.
- o Any Security vulnerability reported by the Bank at any point in time, should be fixed in a time bound manner
- o Security Patches to be provided by the OEM periodically or immediately as necessitated (whichever is earlier)
- o Any Common Vulnerabilities and Exposures (CVEs) in the application to be reported to the Bank, which would be reviewed by the Bank and decide the subsequent course of action.
- o Any Security Incident at the OEM environment should be reported to the Bank immediately.
- o This requirement can be modified or updated subject to Bank's security requirement.

p) Data migration from Bank's existing system should be seamless. Solution provider should have such tools that are time efficient.

q) The Proposed system should be interoperable i.e. it can be integrated with future systems (if required). It should be capable of using AI/ML for predictive risk, fraud detection and SLA optimization.

r) The proposed system must be scalable i.e. in future if 10,000+ vendors need to be added, its performance should not downgrade.

s) The solution provider should be able to update the system as per the prevailing guidelines of regulators i.e. RBI, SEBI, etc. and various relevant acts such as Digital Personal Data Protection Act 2023.

t) Bank's Data Protection Policy to be strictly adhered to and no data should go out of the Bank domain.

u) The solution provider needs to have a Cyber Insurance Policy covering entire gamut of the proposed Third-Party Lifecycle Management System, with proof shared annually with the Bank.

v) Annual third-party security audits of the application must be arranged by the solution provider and reports to be shared with the Bank.

w) A mandatory training for Bank staff/ maintenance team plus refresher sessions every year to be arranged by the developer.

x) Documentation of the proposed application and FAQs to reduce dependency on the developer for maintenance team.

y) Dedicated support team along with escalation matrix needs to be provided for initial 2-3 years.

z) The developer needs to propose one improvement/ innovation clause in its annual improvement plan.

aa) The solution provider to ensure minimum 99.9% uptime of the solution.

The Third-Party Lifecycle Management System will cover the following areas:

- End-to-end management of vendors and their subcontractors, including KYC, due diligence, and onboarding.
- Internal/external Validation on vendors (Viz. PAN/GSTIN/ Adverse media/Litigation history, IBA Caution List, Internal Negative List Portal etc.)
- Creation, monitoring, and breach handling of Service Level Agreements (SLAs).
- Periodic reviews and audits to evaluate vendor performance and compliance.
- Outsourcing Vetting Committee (OVC) for onboarding of activity and review of the same.
- Vendor related Additional details viz. Subcontracting, Financials, BCP, Insurance, Vendor policies, Self-certifications required if any etc.
- Third party Risk Assessment of (Service Provider and its subcontractors) at
  i. Pre-onboarding,
  ii. Onboarding of the vendor
  iii. Periodic Vendor review
  iv. Exit/termination.
- Activity/Sector Specific Third-Party risk assessment and risk assessment at various levels (e.g., ISD will review IT related aspects)
- Identification and auto-escalation of SLA breaches, compliance failures, Penalty for the same.
- Module for Vendor payment and monitoring/management of the same
- Complaints management for the monitoring and resolution
- Handling of Personally Identifiable Information (PII) Data of individuals under Digital Personal Data Protection Act 2023.
- Functionality of recording vendors related frauds.
- Exit/Termination/Blacklisting of the vendor and its employees.
- Comprehensive MIS and dashboards for real-time monitoring and decision-making.
- Role-based access to stakeholders to ensure secure and efficient use of the system.
- Provision for auto scrubbing of negative vendor/ vendor resources data at the time of onboarding a new vendor.

2. USER MANAGEMENT

Stakeholder's Involved
1. Vendor Management Department
2. IT- PR dept.
3. Third Party Risk Management Dept.
4. Information Security Dept.
5. Audit Dept.
6. User Departments at CC/LHO 7. Risk Departments at LHO/CC/BnSG.
8. Vendors Beneficial Owner/SPOC

2.1 Overview

The User Management module defines the roles, responsibilities, and access rights for different stakeholders within the Third-Party Lifecycle Management System. This ensures role-based access control, enhances operational security, and enables efficient management of vendor lifecycle activities.
1. Facilitate role-specific functionality and access rights.
2. Enable centralized creation, modification, and deactivation of user accounts.
3. Automate account lifecycle management using HRMS integration.
4. Notify users of relevant actions via email alerts.

2.2 User Roles and Responsibilities

The Third-Party Lifecycle Management System incorporates a hierarchical role structure with distinct responsibilities for each role.

2.2.1 Super Admin

Responsibilities:
- Full system access across all modules.
- Manage users (create, modify, deactivate).
- Configure system-wide parameters (e.g., activity types, departments).
- Access all reports and documents, such as SLA, due diligence reports, and audit logs.
  Key Actions:
- Generate consolidated MIS reports.
- Override and reassign users if HRMS data changes (e.g., transfers, retirements). Run the updated HRMS API to incorporate the changes.

2.2.2 Circle Admin/ BU Admin

Responsibilities:
- Manage users (Makers and Checkers) within their specific circle.
- Assign users to departments and activities within their jurisdiction.
- View and generate circle-specific reports. *Key Actions:*
- Update user roles based on HRMS data.

- Approve department-specific operations.

2.2.3 Maker

Responsibilities:

- Initiate and create requests for vendor onboarding, SLA creation, and periodic reviews.
- Capture and upload required documents, such as In-Principal Approval (IPA) forms.
  Key Actions:
- Input operational data (e.g., complaints, audit findings).
- Escalate requests for Checker validation.

- Edit rights for the data available in existing fields.

2.2.4 Checker

Responsibilities:

- Validate and approve entries created by Makers.
- Ensure compliance with regulatory and operational guidelines. *Key Actions:*
- Approve or reject vendor onboarding requests and SLAs.
- Suggest corrections or return entries for revisions.

2.2.5 Reviewing Authority

Responsibilities:

- Review and approve vendor and SLA-related evaluations.
- Provide final feedback on audit and review findings.
  Key Actions:
- Approve or reject key decisions.
- Suggest modifications or escalations.

2.2.7 Technical and Price Negotiation Committee (TPNC)

Responsibilities:

- Finalize terms of engagement, modalities of onboarding, viz RFP, Nomination, Pre-Bid meeting, evaluation of vendors on technical and financial parameters.
  Key Actions:
- Upload decisions and meeting minutes to the system.

2.2.8 Risk Management and Audit Teams

Responsibilities:

- Monitor SLA compliance and vendor risk ratings.
- Conduct Periodic Audit. The periodicity of Audit to be defined and alert to be sent to all stakeholders accordingly.

  Key Actions:
- Identify risk and mitigation plans.

2.2.9 Vendors and Subcontractors

Responsibilities:

- Upload KYC and compliance documents. *Key Actions:*

• Respond to queries and update SLA-related inputs.

2.3 Key Features

1. Role-Based Access Control: Ensures users can only access modules and data within their roles.
2. Multi-Role Assignments: A single user can hold multiple roles, such as Reviewing Authority and Circle Admin, based on operational needs. Makers (only) can be linked to multiple departments.
3. HRMS Integration: Automates user account creation, modification, and deactivation based on HRMS data.
4. Automated Alerts and Notifications: Role-specific alerts for tasks like SLA breaches, renewals, and escalations.

2.4 User Creation and Deactivation Workflow

Creation Process:
• Admins create user accounts and assign roles.
• System allots a unique PF ID same as PF from HRMS data. *Deactivation Process:*
• Automated workflows deactivate users based on: HRMS updates (transfers, retirements), Manual admin actions.

2.5 Alerts and Notifications

1. Email & SMS Notifications: Sent to both primary and alternate email IDs and mobile numbers
2. Dashboard Alerts: Highlight pending tasks and compliance requirements.

2.6 Security and Compliance

1. Data Security: Access control ensures users cannot view or edit unauthorized data.
2. Audit Trails: Tracks all user actions for compliance and troubleshooting.

3. MODULES OVERVIEW

Vendor Management Module:
1. Creation of Vendor repository and its management to add/modify/Deactivate.

The following vendor details will be captured during the creation of vendor.
   i. Vendor Type (IT/ Non-IT)
   ii. Name
   iii. GSTIN (Optional)
   iv. Registration No./ Udyam Aadhar no.
   v. PAN
   vi. CIN (if applicable)
   vii. Address

viii. Contact details.

ix. Beneficial Owners' Name

x. Beneficial Owners' PAN

xi. Beneficial Owners' Address

xii. Beneficial Owners' Contact details The same will be applicable for creation of sub-contractors/ sub- vendors.

2. Maintenance of Outsourced Activities and Services- Option for creation, deletion, and modification of Outsourced Activity for both IT & Non-IT.

3.1 Pre-Onboarding Module

The Pre-Onboarding Module facilitates the initiation and approval of vendor onboarding requests. It captures all relevant details and justifications for onboarding a vendor and ensures approvals align with organizational policies.

Outsourcing Vetting Committee (OVC) Module Features:

1. Request initiation by Maker for generation of In-Principal Approval (IPA) form and supporting documents like Approach Paper containing details regarding Department, Circle, Vendor Type (IT/Non-IT), Estimated Budget, Scope of Work etc. Parameters may be changed as per the specific requirements of IT-PR / Vendor Management department. Generation of IPA ID for future tracking.

2. The maker has to select one of the two options- i. Outsourcing of new activity ii review of the activity.

3. Validation of request details by Checkers.

4. Review and approval by the Outsourcing Vetting Committee (OVC) via Easy Approval.

5. Compliance of OVC remarks to be submitted and flow of this module ends here.

Output:

Approved or rejected onboarding to be uploaded. If approved the application is forwarded to next module.

3.2 Vendor Selection Module

This module manages the selection process for vendors using either the nomination or RFP/tendering process.

Features:

1. Allocation of Standing Technical Price Negotiation Committee (STPNC) based on the financial delegation power. *(Option to bypass this step for NON-IT as the process is manual and the approval to be taken through Easy Approval and uploaded in Third Party Lifecycle Management System)*

2. Scheduling TPNC meeting and uploading the MOM in the TPNC Module.

3. Vendor selection methods:

   ⬦ Nomination: Assigns a specific vendor with justification.

➕ RFP/Tendering: Sends requests for proposals and evaluates responses.

4. Generation of unique identifiers:

➕ Nomination ID or RFP ID.

5. Linking of selected vendors to subsequent due diligence processes.

Output:

Selected vendors proceed to the Vendor Due Diligence module.

3.3 Vendor Due Diligence

Ensures that all vendors meet compliance requirements, such as KYC and regulatory checks.

1. Capture of vendor details:

Name, PAN, GST, address, financial documents, etc.

2. Validation through automated APIs:

Income Tax (Protean), RBI compliance, IBA caution list verification and Internal negative list.

3. Scrubbing of directors' data of the Bank and CBS report on Bank employees/ employee family members' data to verify that the proposed vendors or their beneficial owners are not linked to any Bank employee/ their relatives.

4. Automated background checks using NLP (Natural language Processing) to extract insights from external sources (financials, media, legal, regulatory watchlists etc.)

5. Inspection report along with geotagged Selfie of verifying official, verifying Negative Media reports, Litigation History.

6. Creation and Verification of Beneficiary Owners (BOs) as per regulatory guidelines.

7. Unique Vendor ID generation.

Output:

Only verified vendors are allowed to proceed to SLA creation. E-Signature (through digital signature, OTP- based signature etc.) and eStamping of SLA may be included as one of the options in addition to manual signing of the SLAs.

3.4 a. TPRM- Maintenances of Value Statements/Activity/Services-

The risk assessment will be carried out basis the value statement applicable for the activity. Option for creation, modification, and Deletion of Value statement to be provided. For adding value statement, the following set of data will be captured.

i. Vendor Type (IT, NON-IT etc).

ii. Assessment Levels (Onboarding, Review, Exit etc).

iii. Outsourced Activity (e.g.: Doorstep Banking, contact centre etc).

iv. Service (e.g.: For ATM Cash Replenishment, Surveillance, Maintenance etc).

v. Stage (Stages under Assessment Levels).

vi. Activity.

vii. Zero Tolerance (Yes/No). viii. Risk Level.

ix. Risk Type.

b. TPRM- Risk assessment module-

The stagewise risk assessment to be carried out (Vendor and Subcontractors). Provision for arriving at final rating for vendor by clubbing rating of vendor and subcontractors is to be made. Basis the risk assessment various reports to be generated.

Real-time tracking of third-party risk indicators using AI models trained on financials, service data, customer feedback, and external alerts. An Early Warning System is envisaged to predict potential vendor failures or SLA breaches through anomaly detection and trend analysis. Risk related value statements and their respective risk perceptions needs to be defined based on category of vendor and type of activities carried out by the vendor.

3.5 Module for initiating and finalization of the procurement process and functionality for allocation of TPNC and capturing the details.

3.6   Financial Sanction Module (Financial Sanction ID, Budget ID)

i.   The procuring department will ensure that all budget considerations are met before taking the financial approval.

ii.   The system to facilitate automatic checks against the budget for each procurement request according to the procurement estimated cost.

iii.   Generate the Financial Sanction [Financial Amount, Sanction Period, Budget Mapping with the Project, Type of expenditure involved – capex/opex and its subheads] *(Option to bypass this step for NON-IT as the process is manual and the final approval to be taken through Easy Approval and uploaded in Third Party Lifecycle Management*

System) iv. Mandatorily upload the approved Financial Sanction in the system and generation of Financial Sanction ID.

3.6 Purchase Order Generation (PO ID)

1. The PO will be generated once all approvals are received, containing complete purchasing details, including items, quantities, pricing, and vendor details.
2. The PO will act as the reference point for all future procurement actions.
3. For the PO linked with resource hiring, the number of resources onboarded is captured, along with their roles and timelines of the change request.
4. Capture the PO Status – Complete/ Partial (link with ITAM/ ITSM followed by its discovery in the network or lying in the asset inventory/warehouse).

3.7 SLA Creation and Review

Handles the creation, review, and management of Service Level Agreements (SLAs) for vendors and subcontractors.

Features:

1. Creation of SLA templates with details:
   Service description, start/end dates, penalty clauses, KPIs (customizable).
2. The legal team will review and vet the Service Level Agreement (SLA) between the bank and the vendor and Vetting ID generated linked to SLA ID. (Optional for Non-IT).
3. The system will track SLA details, including terms and conditions as defined by the bank.
4. E-mails reminders related to SLA expiry as per the periodicity decided by the Bank.
5. The chain of SLAs (i.e. the original one and subsequent renewals, addendums, extensions etc.) will be maintained in the system.
6. SLA executing department must review the terms (Periodic SLA Review) to assess whether any penalties should be levied based on vendor's performance or resources shortcomings.
7. The penalty, non-performance/shortcomings or any other deductions will be reflected during invoice processing. (For NON-IT option to feed penalty amount along with justification remarks to be incorporated)
8. SLA linking
   Vendor IDs are mapped to their respective SLAs.
9. A digital library of SLAs to be maintained with search option with tracking of all renewals.
10. Once the SLA is executed, the department will enter the SLA in the system capturing details like SLA time period, Contract cost, SLA type – MSA, General SLA, Addendum, SOW, Rate Discovery, SLA Penalty and Target Matrix, Due Diligence etc. (Few parameters not applicable for Non-IT and to be made optional)
11. Option for digital as well as manual execution of SLAs. In case of manual SLAs, upload facility needs to be provided (maximum size of each file should be kept sufficiently high i.e. up to 30 MB).
12. Mechanism for escalation to the mapped Departments such Law, Information Security, Risk etc. be provided, basis various validations/triggers.
13. Different formats applicable to IT, Non-IT and Non-Banking related outsourcing are to be provided in drop-down mode to enable the onboarding depts. to choose suitable format to be used.

Output:

Active SLAs are monitored in subsequent modules for performance and compliance.

3.8 Subcontractor Management

If the Vendor has sub-contracted the service, approval must be obtained and uploaded. Once Subcontractor approval is obtained, proceed for Subcontractor ID creation.

1. Capture subcontractor details.

2. Upload Due Diligence report of Subcontractor as obtained from Main Vendor.
3. Upload suitability evaluation report for the evaluation conducted on the proposed sub-contractor.
4. Upload SLA executed by the Vendor with the Sub-contractor.
5. Mapping of subcontractors to primary vendor SLAs.
6. Automated cancellations of subcontractor SLAs in case of primary vendor SLA expiry.
7. Performance monitoring and reporting for subcontractors.

Output:

Subcontractor review to be done.

3.9 Vendor Resource on boarding (Resource ID) (Optional for Non-IT)

(i) If the vendor provides resources, the system will allow for on-boarding of these resources as part of the PO.
(ii) Auto scrubbing of INL Portal and IBA Caution List at the time of onboarding each vendor resource.
(iii) Each on-boarded resource will be linked to the SLA/ PO with details such as resource's name, role, duration of engagement, and the associated costs.
(iv) Option for removal/ exit of the vendor resources, along with a box for recording the reasons etc. to be provided.
(v) During the resource on-boarding, details like Resource personnel, his/ her qualifications details, Police Verification, Background check, Resource's skill set, price per day as per the billing cycle, Billed/unbilled, backup resource to be captured in the system.
(vi) Vendor exit option should be provided to release the vendor in case of contract expiry or voluntarily exit by the vendor.

3.11 SLA Breach Management

Vendor Score Card

(i) The system will include functionality to periodically assess vendor's performance based on the services provided in alignment with the agreed terms & conditions (as per the SLA/ Contract executed).
(ii) Vendor Score card is done by on-boarding department against the SLA ID associated with the department.
(iii) The SLA targets and score is submitted based on the vendor resource performance on seven parameters namely time, quality, productivity, risk, user satisfaction, innovation, and automation.

Monitors SLA adherence and escalates breaches for corrective actions.

Features:

1. Automated detection of breaches

 Based on KPI metrics and SLA terms.

2. Manually input breaches if found.

3. Escalation workflows:

 Notification to Risk Management and associated departments and Top Management.

4. Penalty calculations and resolution tracking.

5. SLA breach analytics:

 Reports on breach trends by vendor, activity, or region.

Output:

Resolved breaches are archived, while unresolved breaches trigger additional escalations.

3.12 Invoice Processing and Payment (Bill No ID)

- The invoice will be processed based on the PO details.
- Budget details will be verified before the Bill Payment.
- The bill can only be processed within the SLA period/ sanction period. (Deviation to be fed for exception e.g. Valid Bill is submitted after SLA expiry)
- Any penalties identified in the SLA review will be deducted during invoice payment.
- Invoice raised beyond the SLA period/ Sanction period will not be processed in the system. Exception if permitted shall be routed through the controller of the onboarding depts. after duly recording the reasons and permissions.
- Linkage to Banks Vendor payment system (VPS).
- Payment to Active vendors
- Check for Payments must be in line with the contract value.
- Check for Authority structure to make payments.
- Historic data for payments made to the vendor.

3.13 Audit and Review Module

Enables periodic audits and reviews of vendor performance and compliance.

Features:

1. Recording audit findings and corrective actions.
2. Vendor performance reviews based on:

 Cost-benefit analysis, bottleneck observations, target achievements.

3. Risk assessment ratings and compliance tracking.
4. All the SLAs tagged with the outsourcing activity will be subjected to the periodic review exercise.
5. Department needs to submit the Audit, BCP, Testing of BCP and Risk rating parameters related details in the periodic review exercise.
6. Integration of Audit module with the Bank's Third- Party Audit Module.

Output:
Audit and review findings are used for annual evaluations and SLA updates.

Complaint received against vendors

This module shall enable recording complaints received against vendors.
1. Option to feed complaints received against vendors/ sub-vendors is to be provided.
2. Actions taken/ resoluctions provided/ updates on the complaints are to be recorded.
3. Auto escalation of complaints pending for resolution beyond stipulated periodicity to the controlling authority to be provided.
4. Complaints data to seamlessly move for MIS and master dashboard.
5. Module for recording vendor related frauds.

3.14 MIS and Reporting

Provides real-time insights and dynamic reporting for decision-making.
Features:
1.   Dynamic dashboards with filters:
   Vendor name, SLA status, department, circle, etc.
2.   Predefined and custom reports:
   Blacklisted vendors, SLA compliance rates, audit findings.
3.   Drill-down capabilities for detailed data analysis.
4.   Automated report generation and distribution.
5.   List of all procurement
6.   List of details of Re-Tendering
7.   List of Single Vendor Situation
8.   List of EoI
9.   List of OVC
10.   List of RFP
11.   List of PEEC proposals
12.   List of Active TPNC
13.   List of all TPNC
14.   Details of all the TPNC committee
15.   List of procurement through GeM – quarterly and annually
16.   List of all outsourcing activities – quarterly and annually
17.   List of vendors with their SPOCs
18.   TPRA report
19.   Outsourcing activity review report
20.   List of Active SLA
21.   List of all Expired SLA
22.   List of SLA for GRC

23. List of all master SLA
24. List of PO
25. List of all Financial sanction
26. FY wise spending - department
27. List of all master financial sanction
28. List of Bill paid – period wise
29. Amount paid to the vendor - period wise, payment term, SLA wise.
30. List of Bill payment done – IT and NON-IT under project
31. List of Vendors with their PAN, GST for IT and NON-IT procurements

Any other report as and when required/ decided by the bank.

32. Department wise TP-RA assessment details.
33. Bird eye view for Top management /Risk functionaries on Risk Types (Bank/Dept/Circle/BU) wise
34. Vendor wise/Activity wise Risk assessment details
35. TPRA Risk Distribution - Consolidated at Bank level (BU/Circle) along with granular details.
36. ORMD Report - TPRA Assessment Status -wise (Completed, Overdue in cases where SLA is expired, In-progress) - Consolidated at Bank level (BU/Circle)
37. ORMD - TPRA Assessment – Mitigation Plan
38. Various Checks/ Additional requirements:
     Provision to link the new procurement with the chain of existing procurement (in case of renewal to track the procurement history and negotiation process).
39. All the SLAs should be linked with the Old SLA to get the link between the SLAs.
40. The system should be integrated with IT Asset Management (ITAM), IT Services Management (ITSM) etc. Proposed System should be enabled for seamless integration with related system or application that could be introduced by the bank.
41. Complaints against vendors.
42. Audits and their compliance.
43. Business Continuity Plans and their testing results
44. SLA breaches and penalty imposed and recovered.
45. Loss accounted for on account of shortfall in SLA Breach penalty recovered.

4. DETAILED FUNCTIONAL REQUIREMENTS

4.1 Pre-Onboarding Module

1. Request Creation:
       Fields to capture:
   Department, Circle, Vendor Type (IT/Non-IT), Scope of Work, Purpose of Onboarding.

Attachments: Mandatory upload of In-Principal Approval (IPA) form/Approach Paper and justification documents.

Validation: Automatic field validation for completeness and data integrity.

2. Workflow:

Initiation by Maker → Validation by Checker → Review by OVC via Easy Approval.

3. Notifications:

Alerts for pending approvals at each stage.

Outputs:

Approved requests proceed to the Vendor Selection Module. Rejected requests are archived with reasons.

4.2 Vendor Selection Module

1. Nomination Process:

Capture justification for direct vendor nomination.

Assign Nomination ID upon approval.

2. RFP/Tendering Process:

Generate RFP IDs and track submissions.

Upload RFP Approvals.

Evaluate vendors based on predefined criteria.

3. Committee Review:

Integration with TPNC for decision-making.

Upload and link Meeting Minutes of TPNC.

4. Notifications:

Status updates to stakeholders.

Outputs:

• Selected vendors proceed to the Due Diligence Module.

• Non-selected vendors are archived for future reference.

4.3 Vendor Due Diligence

Functionality:

1. Data Capture:

Vendor details: Name, PAN, GST, address, financial documents.

2. Verification:

Automated checks using APIs (e.g., GSTN, PAN OPV, RBI compliance, IBA Caution List, Internal Negative List Portal).

Validation of Beneficiary Owners (BOs) as per KYC norms.

Generate unique Vendor IDs upon successful verification.

3. Notifications:

Alerts for missing or incomplete documents.

Updates on verification status.

4. Handling PII Data - implementing security measures, following regulatory requirements, and establishing procedures to protect personal information from unauthorized access, misuse, or breach.

5. Functionality for recording vendors related frauds.

4.4 SLA Creation and Review

Functionality:
1. SLA Templates:
 Predefined templates for primary and subcontractor SLAs.
 Fields: SLA ID, service description, customizable KPIs, penalty clauses, start/end dates.
2. Review and Approval:
 Workflow: Maker → Checker → Reviewing Authority.
 Integration with Risk Management for high-value SLAs.
3. Automation:
 Auto-reminders for SLA renewal and periodic reviews.
 Auto-linking of Vendor IDs to SLA IDs.
4. Penalty Calculations:
 Real-time penalty calculation for SLA breaches based on breach metrics.
Outputs:
- Active SLAs are monitored for compliance.
- Archived SLAs are retained for reference.

4.5 SLA Breach Management

Functionality:

1. Monitoring:
 Automated tracking of SLA performance against KPIs.
 Highlight breaches based on predefined thresholds.
2. Escalation:
 Notify Risk Management and relevant stakeholders of breaches.
 Trigger corrective action workflows.
3. Resolution Tracking:
 Log corrective actions, responsible staff, and deadlines.
 Update breach status (Resolved/Pending).
Outputs:
- SLA breach logs for audit and analysis.
- Escalation reports for unresolved breaches.

4.6 Audit and Review Module

Functionality:
1. Audit Scheduling:
 Create schedules for internal and external audits as per periodicity decided.
 Link audits to specific vendors, activities, or SLAs.

2. Review Process:
 Capture observations, corrective actions, and compliance ratings.
 Upload supporting documents (e.g., audit findings, review reports).

3. Risk Assessment:

Assign risk ratings based on audit findings.

Escalate high-risk issues to Risk Management.

Outputs:

- Detailed audit reports for vendors and activities.
- Risk ratings and recommendations.

4.7 Subcontractor Management

Functionality:

1. Subcontractor details capture: Name, parent vendor ID, registered address, linked SLA documents.
2. Due Diligence to be done by Main Vendor after getting the approval from Department concerned.
3. Subcontractor Linkage:

Link subcontractor SLAs to primary vendor SLAs.

Ensure cascading compliance with SLA terms.

4. Notifications:

Alerts for subcontractor SLA renewals or breaches.

5. Subcontractor ID to be created.

Additional data (Input module may be given to Vendor (User from vendor) with document upload facility)

- i. Subcontracting Details
- ii. SLA data (Contract value/Period etc.)
- iii. Financials of Vendor
- iv. BCP plan/ Contingency plan/ Testing etc.
- v. Insurance
- vi. Self-certifications required if any.
- vii. vii. Vendor Policies required if any.
- viii. Digital execution of SLAs.

TPRM assessment by the department concerned

E.g., I.S. related checks should be verified from ISD

Module for Vendor Termination/ Exit /blacklisting of Vendors / Vendors employees

1. In cases of terminations/ exit of the vendor, option for upload of NOC and Data Purging Certificate to be provided at vendor as well as onboarding department end.
2. Functionality for recording transfer of ownership of the Bank's assets to the vendor onboarded in place of outgoing vendor to made available.

5. REGULATORY COMPLIANCE AND RISK MITIGATION

5.1 Objectives of Compliance and Risk Mitigation

1. Ensure adherence to external regulatory guidelines (e.g., Reserve Bank of India [RBI]).
2. Automate compliance checks to reduce manual errors.
3. Provide real-time alerts for potential non-compliance.
4. Mitigate risks by integrating checks into workflows like onboarding, SLA creation, and audits.

5.2 Key Compliance Features

5.2.1 Regulatory Framework Integration
- RBI Guidelines: Adherence to outsourcing rules for financial institutions.
- KYC Compliance: Vendor and subcontractor identification using PAN, GST, and Aadhaar.
- Blacklist Validation: Automated checks against IBA and internal blacklists.

5.2.2 Automated Due Diligence
- Verify vendor credentials during onboarding and SLA creation.
- Conduct financial stability checks using uploaded documents like financial statements.
- Link compliance results to SLAs for SLA-specific monitoring.

5.2.3 Audit Integration
- Record and track audit findings, corrective actions, and risk ratings.
- Ensure compliance gaps are escalated and addressed.

5.2.4 SLA Monitoring
- Real-time SLA performance monitoring.
- Escalation of SLA breaches with pre-configured penalty clauses.
- Link SLA reviews to vendor risk ratings.

5.3 Risk Mitigation Features

5.3.1 Risk Assessment during Onboarding
- Assign risk ratings based on due diligence outcomes to be done by RISK Department
- Highlight high-risk vendors for additional scrutiny during SLA creation.

5.3.2 SLA-Specific Risk Management
- Identify risk-prone SLAs (e.g., high-value, critical operations).
- Track and resolve breaches linked to risk ratings.

5.3.3 Subcontractor Risk Tracking
- Enforce cascading compliance for subcontractors linked to high-risk vendors.
- Terminate subcontractor SLAs if primary vendor fails compliance checks.

5.3.4 Escalation Mechanisms

• Automated notifications to Risk Management and Admins for:
• SLA breaches.
• Audit findings requiring immediate action.
• Regulatory lapses detected during periodic reviews.

5.4 Real-Time Alerts and Notifications

Triggered Alerts:
1. Missing compliance data during onboarding (e.g., PAN or GST validation failures).
2. SLA breaches exceeding predefined thresholds.
3. Expiry of critical documents like SLAs or audit certifications.
4. Automated Escalation to Risk departments.

5.5 Compliance Reporting

Key Reports:
1. Vendor Compliance Report:
 Tracks KYC status, blacklist checks, and financial verification.
2. Audit Findings Report:
 Summarizes audit results, risk ratings, and unresolved issues.
3. SLA Compliance Report:
 Details SLA performance, breaches, and penalties.
Regulatory Submissions:
 • Generate compliance reports in formats required by regulators (e.g., RBI).

5.6 Risk Mitigation Workflow

Workflow: SLA Breach Resolution
1. System detects a breach (e.g., missed KPI).
2. System sends alerts to Risk Management Team.
3. Risk Management investigates and logs corrective actions.
4. Stakeholders monitor the resolution or escalate unresolved issues.

5.7 Security and Access Controls for Compliance

 Role-Based Access Control (RBAC): Ensure only authorized users can modify compliance-related data.

6. CONCLUSION

The Third- Party Lifecycle Management System aims to address the critical need for transparency, compliance and efficiency in Vendor Management. By automating key aspects of vendor management as shown above the system will ensure adherence to regulatory guidelines while facilitating seamless coordination among departments and stakeholders.

6.1 Disclaimer

Brief overview of the proposed procurement/scope of work given in this document may be further elaborated, viz., more details may be included in the Request for Proposal (RFP) document to be issued post EOI.

Appendix-D

Bidder Details

Details of the Bidder

S. No.	Particulars	Details
1.	Name	
2.	Date of Incorporation and / or commencement of business	
3.	Certificate of incorporation	
4.	Brief description of the Bidder including details of its main line of business	
5.	Company website URL	
6.	Company Pan Number	
7.	Company GSTIN Number	
8.	Particulars of the Authorized Signatory of the Bidder a) Name b) Designation c) Address d) Phone Number (Landline) e) Mobile Number f) Fax Number g) Email Address	

Name & Signature of authorised signatory

Seal of Company

Appendix-E

Pre-Bid Query Format

(To be provide strictly in Excel format)

Vendor Name	Sl. No	EOI Page No	EOI Clause No.	Existing Clause	Query/Suggestions

Appendix-F

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)	

Appendix–G

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 _____ 2025 , 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:

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.

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.

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.

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 if 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 completion of reverse auction 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.

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.

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.

Independent Monitors

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

Shri Otem Dai	Shri Satyajit Mohanty
otemdai@hotmail.com	satyajitmohanty88@gmail.com

7.2 The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.

7.3 The Monitors shall not be subjected to instructions by the representatives of the parties and perform their functions neutrally and independently.

7.4 Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings. Parties signing this Pact shall not approach the Courts while representing the matters to Independent External Monitors and he/she will await their decision in the matter.

7.5 As soon as the Monitor notices, or has reason to believe, a violation of this Pact, he will so inform the Authority designated by the BUYER.

7.6 The BIDDER(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the BIDDER. The BIDDER will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor shall be under contractual obligation to

treat the information and documents of the BIDDER/Subcontractor(s) with confidentiality.

7.7 The BUYER will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the parties. The parties will offer to the Monitor the option to participate in such meetings.

7.8 The Monitor will submit a written report to the designated Authority of BUYER/Secretary in the Department/ within 8 to 10 weeks from the date of reference or intimation to him by the BUYER / BIDDER and, should the occasion arise, submit proposals for correcting problematic situations.

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.

Law and Place of Jurisdiction

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

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.

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   Authorized 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.