



**Request for the Proposal for Supply, Installation, Customization,
Implementation, Integration, Training, Support and Maintenance of Audit
Management Solution for Risk Based Internal Audit
in THE KERALA STATE CO-OPERATIVE BANK LTD (KERALA BANK)**

**In Collaboration With
KERALA STARTUP MISSION**

Reference No. KB/IT/AMS/KSUM/07/2026 Dated 22-06-2026

Table of Contents

SL #	Particulars	Page #
	SECTION: I - SCOPE OF WORK	
1	Scope of RFP	4
1.1	Details of Scope of Work	4
1.2	Audit Management Solution	5
1.3	Units covered by Audit	8
1.4	Procedure for Audit Activity	8
1.5	About Audit Management Solution (Technical & Process Flow)	8
1.6	Offsite Monitoring System (OMS)	12
1.7	Objective for Implementing Off-Site Monitoring System	12
1.8	Scope for Offsite Monitoring System	12
1.9	Scope for Exception Management	13
1.10	General Aspects in Scope	13
1.11	Training	15
1.12	Locations for work	16
1.13	Timeline for Go-Live	16
1.14	Attendance Report for Inspecting Officers	16
1.15	Interface and Integration Requirements	16
1.16	Disaster Recovery Mechanism	16
1.17	Implementation Methodology	16
1.18	Functional Gap Specification Study	17
1.19	Customization	17
1.20	Gap Identification and Resolution	17
1.21	UAT	18
1.22	Infrastructure (Hardware/Network)	18
1.23	Audit	18
1.24	Procedures in place to periodically test the backed-up data	19
1.25	Installation on existing or new setup	19
1.26	Upgrade the proposed solution	19
1.27	No unwarranted, illegal, and fraudulent misuse of data	19
1.28	Support for the present and future proposed interfaces	19
1.29	Support applicable as and when released by the OEMs	19
1.30	Maintenance Support	20
1.31	Facility Management	20
1.32	Artificial Intelligence Compliance Requirements	20
1.33	Compliance to Digital Personal Data Protection (DPDP) Act 2023	22
1.34	Software Bill of Materials (SBOM)	22

	SECTION: II GENERAL CONDITIONS OF CONTRACT AND SERVICE LEVELS AGREEMENT	Page #
2.1	General	23
2.2	Term and Extension of the Contract	24
2.3	Warranty	24
2.4	Prices	25
2.5	Payment Terms and Schedule	25
2.6	Service Level Agreement & Targets	26
2.7	Quality & Cost Based Selection (QCBS)	26
2.8	Integrity Pact	26
2.9	Liquidated Damages (LD)	26
2.10	Eligibility Criteria	27
	Functional Requirements	28

SECTION : 1 – SCOPE OF WORK

The Kerala State Co-operative Bank Ltd. (KSCB)

The Kerala State Co-operative Bank is the Apex bank in the Co-operative credit structure of the State of Kerala. The 14 District Co-operative Banks in the state have been merged with the Kerala State Cooperative bank which formed a single entity having 823 branches across Kerala with the brand name “Kerala Bank”.

I. Scope of RFP:

The objective of this RFP envisages an end-to-end comprehensive solution for conducting Risk Based Internal Audit (RBIA) according to the latest guidelines issued by various regulators and Bank policies & guidelines. Details of Scope of work is mentioned in Section 1.0/1.1

The solution should have the following key attributes:

- Provide basis for risk scoring of the auditee units based on evaluation of their risk profiles, comprising of Business risk and control risk procedures and results of any substantive audit tests / procedures performed by the auditor.
- To enable the internal audit to serve as an independent, objective assurance and consulting activity

1.0 The Bank intends to adopt a **configurable technology platform layered Audit Management Solution above Core Banking System (CBS)** instead of a standalone audit module.

- The solution shall act as an **enterprise audit and inspection platform**, supporting:
 - Risk Based Internal Audit
 - Concurrent audit
 - Compliance audit
 - Inspection, vigilance, etc.
- The platform should be:
 - **API-driven**
 - **Event-driven (real-time / near real-time)**
 - **Configurable**
- It must act as a **unified Governance, Risk & Audit layer** integrated with:
 - Core Banking Solutions
 - Loan Origination System
 - Early Warning System
 - Other enterprise systems if any

1.1 Details of Scope of Work

The detailed Scope of Work of this RFP envisages an end-to-end comprehensive solution for Audit Management Solution, Onsite and Offsite Monitoring System, which includes procurement of perpetual license & Supply, Installation, Implementation, Integration, Maintenance and support of the Solution and other components required, along with parameterization, historical data management, verifying data quality, user acceptance testing, documentation, training, knowledge transfer and support.

The proposed solution should be scalable so as to support legacy applications if any, used by Bank or be capable to integrate Bank’s other Projects in the future as Bank may go for up-gradation, at a later date. This would also

envisage parameterization, historical data management, verifying data quality, user acceptance testing, documentation, training, knowledge transfers and support.

1.2 Audit Management Solution

A. Type of Audit

Risk Based Internal Audit (RBIA)

- a. Phase I : Branch Audit
- b. Phase II : PACS / Other Societies Audit
- c. Phase III : Audit by Regional Operations Managers

B. Aspects to be covered by Solution

2. The system should be able to accommodate **functionality of audit** at the Branches, CPCs, Regional Offices, CBO, PMU, Head Office Departments, PACS / Other Societies etc
3. System should provide **workflow facility for Audit Life Cycle management** which includes **audit planning, execution, report preparation, closure, management reporting**, etc.
4. The proposed software should be able to **identify and keep track of all auditable units/branches** of the bank.
5. The System should be able to address the following dimensions.
 - a. **Pre-Audit** requisite for auditor
 - b. **Grouping** of Products, Services, Processes
 - c. Identification & categorization of **risks as High/Medium/Low**.
 - d. Implementation of **Audit Plan based on Risk Category**.
6. The system should enable **pre-configured templates** relating to Business Risks, Control Risks, Operational Risk, Credit Risk, etc. Templates will be shared with successful bidder. Also, addition/deletion/modification in any of the formats will be decided by Bank. Number of templates may vary as per requirement of the Bank. Bank should be able to change in formats / templates in the system by Bank's official.
7. **User Maintenance** – There should be secured user administration in the application. Access and permission to each user to be confined strictly to the respective roles, as defined by the Bank.
8. System shall maintain and update the **branch profile i.e. category, risk profile**, etc.
9. **Customization** will be as per the Bank's requirement and it should conform to the latest guidelines issued by the various regulators and Bank policies and to be adapted as per need of the bank, which is dynamic in nature.
10. Risk assessment by the software should not only indicate the **level of risk as Extremely High, Very High, High, Medium and Low but also the trend of risk** in terms of increasing, decreasing or stable/Risk movement and analysis.
11. The system should enable the Bank to prepare a **Risk Audit Matrix** which would be based on the control risk and business risk.
12. System should have: **Automatic generation of risk rating / matrix** and suggested audit frequency as per Bank's Policy, the Business Risk is based on quantitative data uploaded/fed into the application and Control Risk is calculated as per onsite audit process in the application.
13. Provision to **downgrade/upgrade business risk/control risk status at HEAD OFFICE** and generation of log history for the same should available.
14. System should have option to **generate Inspection plan at HO** based on the previous Inspection rating and the

Bank's policy on frequency of audit (with a provision to reschedule the inspection in case of need). System should have option at HEAD OFFICE to assign & schedule / reschedule / Modify schedule RBIA of a branch/ PACS / Other Societies

15. Inspection scheduling based on the availability of Inspectors and the Bank's audit plan. **Assignment of audit to a team of Inspectors can be done through the application.**
16. The system should **allow any number of auditors** to be tagged to each auditee for the purpose of audit. Like, audit can be handled by a single auditor or team of auditors. In case of more than one auditor, one of them will be designated as leader.
17. **One Auditor can continue at more than one branch / PACS / Other Societies for RBIA** at given point in time. Also, One Auditor can continue more than one audit (other than RBIA) at given point in time.
18. The system should be able to allot **man-days** as per user's requirement. Automatic calculation of man days taken for inspection against man days allotted
19. The system should store the status regarding various **inspection reports such as open, closed, partial rectification, closed with open items**. Bank should be able to define such parameters.
20. **Automated data extraction of Audit Data from various systems** available with the bank. Audit data – it can be extracted from various IT system available in the Bank such as **CBS, LOS, MIS reports or other systems or manually prepared by the auditor** at the site which is a part of the report. At the start of audit, the data shall be pulled from CBS, LOS or other system to AMS (Audit Management Software) in one step.
21. **Automatic sampling of loan accounts** to be considered under current RBIA as per Bank's policy which is updated from time to time. There should be provision for an auditor to **manually add / select an account if he identifies observation / irregularity in account** which is not included in above sample list or if he wants to audit few more accounts.
22. The **Bank should be able to create any types of Inspection** with suitable check list as per changing needs / requirements. Any changes in format or check list should be easily available in the software by the Bank's team.
23. **Audit observations** are in 3 types,
 - i. **Observation**
 - ii. Positive **confirmation** – certificate
 - iii. Adverse remarks – **irregularities** which require compliance.
24. The RBIA report will be discussed with the Auditee before finalization. There **should be a provision in the system to generate the reports on irregularities to auditee during the course of Audit on daily basis** to enable about the spot rectification of the observed irregularities by branches.
25. **Immediately after finalization of RBIA** by the Internal Inspector, it should be made **available to HEAD OFFICE/Regional Office** along with summary report. Inspection report after approval of HEAD OFFICE should be issued to respective Auditee / RO / HEAD OFFICE as required along with summary report.
26. **Audit report** to be made available **online** to the Branch/respective offices. **Auditee should be enabled to give reply online to the RO to accept or reject** with comments and confirm completion of compliance.
27. **Intimation of observations to authorized official/s of the branch / PACS / Other Societies for initiation of spot rectification by Email / SMS** on generation of report by Auditor.
28. **All branches / Auditees will be required to submit rectification of major / other observations / irregularities within a specified time** as per policy of the Bank. The system should generate e- mail reminders to the Auditees / ROs / HO Departments.
29. The HO/RO shall **examine the rectification report and will either accept or reject** it with comments. Auditee can re-submit the rectification.
30. **Display of Observations / Irregularities with Inspector's comments, branch reply, spot rectification details with date** etc., for the authorized Officers at RO to decide to close any inspection observations / report or to raise follow up query against any of the point.
31. **Provision for Inspection report closure as per Bank's norms**. HO / RO Office should have menu to issue

Closure Certificate after

- 100% compliance of all irregularities / observations OR
 - The closure is approved by Audit Committee of Executives (Committee comprising HEAD OFFICE for taking closure decisions)
32. **The observations / irregularities not accepted by Regional Office** will be available for recording further replies till the inspection report is closed. All Observations / irregularities which are unrectified at the closure of inspection should be carried over as Persistent Irregularities in next Audit Report.
33. **Facility to report Income Leakage identified during RBIA** with details like area, account number, amount, etc. This has to be signed by Inspecting Officer and Branch Manager / Auditee Head.
34. Documents upload Facility, so that **authorized user can float confidential documents like Special Reports/Investigation Reports etc.**, marked to specific users through the system and would be instantly and confidentially available to the specific users while they login to the system.
35. **Offline** (upload facility) for comment / Observation / irregularity is required for RBIA audit module.
36. Audit Software should support **Malayalam** language.
37. **Instant Generation of Risk Assessment Matrix, trend analysis report after branch inspection.** This can be generated operational area-wise under Business Risk/Control Risk Classifications
38. **Any report on any irregularity / risk status or branch efficiency on any operational area** in respect of any of the previous Inspection of any Auditee should be instantly generated.
39. The system should be able to **generate letters / e-mail for the communication of rating by RO / HEAD OFFICE to the branches.** The system should store the ratings. It should be possible to store the ratings of earlier years also and generate various types of the reports based on the ratings. The Controlling offices should be able to generate reminders through letters/emails/SMS etc. in respect of branches / Offices where Inspection reports are pending. This should be for Branches coming under respective Controlling Offices.
40. **Complete Inspection Cycle and Historical Data maintenance matching with Bank's Inspection process flow cycle and reporting formats** is to be captured in the system. The whole process of capturing of legacy data shall be completed by the time of go-live. File upload in structured format be provided.
41. The **transfer/upload of the legacy data** into the solution compatible file structure shall be the responsibility of the bidder.
42. System should **support alert and escalation mechanism** by way of SMS and Email for various events / milestones as required / defined by the bank. There should have an **option for immediate escalation of incidents by the Auditor**
42. **Provisions** for Loan Review Mechanism (LRM), Credit Audit, Self-Audit, Surprise Audit, Concurrent Audit, Income & Expenditure Audit, Transaction Process Audit, Revenue Audit & KYC Audit forming part of RBIA Module.
43. **Reports** to be generated:
- a. **Summary** Report
 - b. Region-wise report on Branches **under Audit for specified date range**
 - c. Region-wise report on Branches **with completed Audit for specified date range**
 - d. Region-wise report on Branches **outstanding for closure for specified date range**
 - e. Region-wise report on Branches **with irregularities with risk rating**
 - f. **CPC-wise or Area-wise** report on Branches with irregularities open / closed with risk- wise.
 - g. List of branches **overdue for inspection**
 - h. **Trend Analysis** for Risk Rating.
 - i. Region-wise Branch-wise **list of persistent irregularities**
 - j. Region-wise list of **High/Medium/Low**
 - k. **List of inspection carried out by particular Inspecting Officer in specified date range**
 - l. **List of inspection carried out by Inspecting Officers in the HEAD OFFICE in specified date range**

- m. **Income Leakage** identified Branch-wise / Region-wise
- n. Ad-hoc reports
- o. Abnormality report
- p. Incident flash/special report/s

1.3 Units covered by Audit

- a. HO Departments, Regional Offices, Branches, Other Offices of the Bank (CPCs, CBO, PMU)/ PACS / Other Societies

1.4 Procedure for Audit Activity

- a. Type of roles for login credentials
- b. Checklist / Questionnaire during audit activity, inputs captured to be freeze
- c. Supervisor allocation of audit
- d. Allocation – Reallocation for audit
- e. Audit execution
- f. Maker – Checker concept
- g. Auditee Compliance
- h. Maker – Checker concept – approval process
- i. Auditor Remarks & observations

Audit Management process involves managing the complete audit lifecycle - from development of standard audit checklists, audit planning and scheduling, audit execution, development of audit reports and recommendations, audit compliances, review by Auditees and Management, and implementation of audit recommendations.

1.5 About Audit Management Solution (Technical & Process Flow)

The proposed solution and automated audit tool should take care of end-to-end audit process, to provide a risk-based audit report, based on control and inherent business risk. The Audit Automation Software should help The Kerala State Co-operative Bank Ltd (Kerala Bank) to manage a wide range of audit-related activities and processes in a single and comprehensive framework. This Solution should provide the flexibility to support all activities pertaining to Internal Audit. The solution should provide a single framework for all audit activities and support complete Audit Lifecycle Management.

Technical Functionalities

1. Dynamic Audit **Checklist Creation**
2. Facility for **Risk based Audits**
3. **Planning** and **Scheduling** of Audits
4. **Resource** Allocation / Re-Allocation
5. **Maker Checker** based Workflows
6. Trigger **Event** based Alerts

7. **Account / Product** based sampling
8. Facilitate recording of Audit observations for **particular functional area**
9. Generation of **Rating** Sheet
10. **Workflow based** submission of Audit Compliances & Closure
11. Masters for **configuration of Audit Parameters** Supports organization's governance and risk management policies
12. Strengthening the efficiency of the audit staff, enabling them to be focused on **value-oriented functions such as analyzing and recognizing trends** in the audit data
13. **Standardization** of the Audit Process.
14. **Reduction in the time and effort** involved in preparing for and conducting audits.
15. **Systematic and workflow driven audit** processes across the enterprise with standardized data collection **to eliminate audit errors and inconsistencies**
16. Provision of complete visibility into audit processes and metrics for **better risk management and assured compliance.**
17. Facility of closed-loop **audit cycle** for recording findings, developing recommendations, and implementing action plans.
18. Tracking of **Pending irregularities.**
19. **Single and Centralized Repository.**
20. **Reduction in time** to conduct Audit
21. **Reduction in costs** associated with the audit processes
22. Provision of fully configurable assessments that reveal the **inherent business risk and control risk** associated with each type of audit and entity.
23. Provision of flexible **reporting and dashboards** for enhanced visibility and faster decision making.
24. **Security management of all information** in a centralized, scalable and reliable system

Process Flow

1. Master **Creation**
2. Audit **Checklist** / Format Creation/Accounts & product-based sampling
3. Audit Planning / **Scheduling**
4. User **Mapping**
5. Supervisor **Allocation** / Re-Allocation
6. Resource Allocation / Re-Allocation (Auditor)
7. Audit **Execution**

8. **Rating** Sheet, Income Leakage
9. Audit **Report** Release
10. Auditee **Compliance** Submission
11. **Compliance** Approval
12. Audit **Closure**
13. **Work in Progress** (WIP) Auditee and Approval
14. **MIS** Reports

Business Criticality

SL No.	Business Criticality	Requirement Description
1.	H	Automation of Planning
2.	H	Scheduling & resource allocation for all types of Audits
3.	H	Generation of Rating Sheet
4.	H	Dashboard view and MIS Reports
5.	H	Facilitating Audit Closure
6.	H	Tracking Module to the HEAD OFFICE is utmost important as per RBI Directives.
7.	H	Read the excel sheet generated by the solution in AMS at the time of Audit execution
8.	H	As per the Audit Policy of the bank, business risk is considered for assessment of overall audit risk of the Branch. Audit Management Solution (AMS) should be able to derive business data (Deposits & Advances) from Finacle for annual audit plan. As per the internal guidelines, audit ratings are finalized based on the business risk & control risk (i.e. overall business data of the branch) by HEAD OFFICE. Therefore, AMS is to derive business risk & control risk and make available the report at the appropriate level for final vetting of audit rating.
9.	H	Incorporation of branch compliance approval process as defined in the RBIA Policy, with regard to intervention of HEAD OFFICE for vetting branch compliance reports, based on the size of the business of each branch.
10.	H	Final Audit Closure Certificate (FACC) edit option would be enabled for Head Office and system will allow Branch Head to provide compliance till the FACC issues are fully complied with. Internal Auditor/Audit Supervisor's comment on rejection of FACC/Compliance will be visible to auditee/Branch.

H – Highly Critical

Multiple Login Credentials:

SL.NO	Role Name	Responsibility
1	Super User (HEAD OFFICE)	User Authentication, Execution Format, Masters, Audit Planning, Supervisor Allocation
2	Administrator at HEAD OFFICE	Masters, Execution Format, Dashboard View, MIS Reports, Upload Documents, Audit Cancellation, Audit Calendar, Branch/Area Assignment
3	Audit Controller at HEAD OFFICE	Key Audit Finding, Compliance Alert, Upload Document, Send Mail, Monitoring Process, Send Mail, Compliance, Audit Closure, View Audit Workings, Resources, Approvals, Area Assignment
4	Audit Supervisor at ROs	View Audit Workings, Resources, Comments of RO on Audit Reports, Upload Document, Send Mail, RO observations/FACC
5	Branch Head	Auditee Observations
6	Internal Auditor	Audit Execution, Leave Details, Audit Working

1.6 Offsite Monitoring System (OMS)

As a part of the scope of work, the Vendor need to supply, implement, and manage the Off- Site Management Solution along with Exception Management which will **help to manage the Risk through continuous monitoring of audit exceptions as an offsite monitoring exercise**, on near real time basis.

1.7 Objective for Implementing Off-Site Monitoring System

The Proposed Solution should fulfill the following Objectives of The Kerala State Cooperative Bank Ltd (Kerala Bank):

1. Better **Risk Management through continuous monitoring of audit exceptions** as an offsite monitoring exercise, on near real time basis
2. Provide an **opportunity for timely rectification** of irregularities and minimize the risk
3. **Reduction of the onsite audit workload** and thereby reduction in cost
4. Provision of **facility for Branches to update the status against** each exception
5. **Fraud indicators & Trend Analysis**
6. **Compliance Monitoring**
7. **Transaction Analysis**

1.8 Scope for Offsite Monitoring System

1. Proposed Solution should be **useful for RBIA**
2. The Solution should capture **relevant data from Core Banking** or other systems to generate rule-based exceptions.
3. **Monitoring** of critical and pending issues, Audit trail generation of various MIS reports, Dash board with drill down, and analysis of the data.
4. AMS should be able to **upload identified reports from CBS** for audit & inspection purposes as and when required.
5. **Placing reports/notes before the Top Management** in respect of major findings/ irregularities, status of compliance, monitor able action plan, etc.
6. Compilation of **summarized notes** containing detailed information on irregularities observed progress in rectification, and the risk level of regions for placing to the Top Management /Audit Committee of Board and Board of Directors
7. The Solution should **generate exceptions** on near real time basis as per pre-defined periodicity.
8. The Solution should have the capability to provide **additional Rules** as per user requirement.
9. The Solution should have the **Provision for Exception Management through distribution matrix**.
10. The Solution should have the **Capability to provide drill down to analyze** the exception
11. Solution should provide chance for taking immediate **corrective action to avert any possible damage**.
12. There must be a facility available in the system for **branches to record rectification of irregularities / status updating, based on which Controlling office** can take a stand for closure of the case.
13. Alerts should be generated as per Bank's defined rules and categorized under **High/Medium/Low category**.
14. Solution should have the ability to generate alerts categorized as **High/Medium/Low**.
15. Solution should have the ability to generate alerts **assigned to Branch/RO/HO as per rules**
16. **Evidence/comments be submitted by Branches**.
17. The Solution should have the capability wherein **RO/HO can accept/reject with comments for rejected alerts. Resubmission should be allowed**.
18. All risk (High, Medium, Low) **alerts will be closed at HEAD OFFICE/Regional Office** on the basis of

RO/Branch comments.

19. **HEAD OFFICE can accept/reject with comments for rejected alerts.** Resubmission should be allowed.
20. **User management** for HEAD OFFICE/RO/Branch level etc.
21. Solution should provide **Statistical reports** on alerts:
 - a. **Age-wise** pendency
 - b. **Category-wise** pendency
 - c. **Closed**
 - d. Branch/CPC/RO/HO **level** reports

1.9 Scope for Exception Management

1. The Solution should distribute the **exceptions** to Branch / RO / Audit Department with specific work flows, as per user requirements
2. It should have facility for the **Reviewing** authority to Reject / Resend the exceptions to branch where rectification is unsatisfactory
3. The solution should provide access to system to Concurrent / Internal Auditors, for **information / physical verification**
4. System should provide for **Closure** of the exception
5. Should have the facility to archive the exceptions where rectification of irregularity is completed
 - **MIS:** The Solution should provide Branch-wise, age-wise report on unattended / uncertified exceptions
 - **Dashboards:** Comprehensive dashboard with graphics to be provided for Audit Dept., Controlling Offices.

1.10 General Aspects in Scope

It shall be the sole discretion of the Bank and the vendor shall not have any rights to claim the availability of PCs. Regarding hardware provided by the Bank if any, any installation of software/ tool or any change in the configuration should have prior approval from the Bank.

In brief, the expectations from the bidder will be–

1. The proposed solution should **maintain logs and audit trails** of all the activities. The audit logs should be capable of being used for forensic evidence. Being a financial institution, Bank expects that the proposed solution should facilitate necessary security check and validation processes for ensuring fool-proof access to the systems. These security measures should be an integral part of the proposed solution.
2. The selected Bidder should provide **one year of comprehensive warranty for proposed solution** including associated services **after completing Proof of Concept (POC) for the proposed solution**. The warranty of the proposed solution will start from Go-Live Date of the proposed solution. After the completion of One year of warranty, the Bidder will maintain the software **for 4 years** (plus extended period, if any) as a part of **ATS**. The comprehensive charges for 5 years including one year of Warranty period and 4 years of ATS Period would form part of TCO (Total Cost of Ownership).

3. **Multiple levels of authority** are mandatory so that the proposed solution can provide multiple levels of access for users, managers, administrators etc depending on their roles.
4. Any **security related** issues (including various audit conducted by the Bank/Third Party) reported/observed in the system is to be rectified on top priority. The Bidder is required to fix any vulnerability in the proposed solution at no additional cost during the entire tenure of the contract.
5. The successful Bidder **should take care of all aspects of installation on existing or new setup, De-Installation, Configuration, Re-configuration, enhancements, updates, version upgrades, problem analysis, on-site as well as off-site support** to ensure smooth operations during and post implementation on perpetual basis.
6. The scope of the services is to be provided for the project **duration initial for 5 years** with an option to the Bank to **exit after 90 days' notice** (Services will be deemed to have been implemented from the Go-Live date i.e. from the date when bank decides to live the software for the end users).
7. Project Completion Document should be comprehensive to enable the bank to refer to any details at a future date in case of faults/errors or maintenance/upgrade /patch management.
8. The **Bidder should develop new Reports to modify/ combine existing reports** as per instructions/ requirements from RBI/Bank, etc. during the whole contract period of 5 years.
9. **Bank conducts VAPT (Vulnerability Assessment & Penetration Testing)** and Information Security audit on quarterly basis. The Bidder/ OEM needs to comply with the findings of the VAPT/IS Audit/Secure Coding Practices in terms of the proposed solution provided under this RFP.
10. The successful Bidder has **to meet the requirement of CISO** before going Live since approval of CISO is mandatory. The Bidder has to resolve any VAPT/External/Internal/RBI Audit observations within stipulated time.
11. The successful Bidder is expected to **maintain coding standards** as per best industry standards and bank reserves the right to audit the source code for industry standards.
12. **The Bidder is expected to develop a disaster recovery plan for restoration of the system** in the event of any disaster or major incident. The Disaster recovery plan will be first tested prior to go-live to verify DR readiness and then on every subsequent DR Drill conducted by Bank. The Bidder shall support during the DR drill and period will be decided by bank.
13. **Bidder will provide Application interface architecture for application network.**
14. **Bidder will ensure secure code review post** major/critical changes to the application/software
15. The **Bidder shall have an escrow arrangement for the source code** for ensuring continuity of services in case the vendor defaults or is unable to provide services. Cost towards Escrow arrangement should be a part of Commercial
16. Bidder will **provide Source code** audit certificate.
17. Bidder will ensure **Audit trails** should be enabled for application server.
18. **Bidder will provide Data Flow Diagram** for Application.
19. Bidder should provide duly signed Non-Disclosure Agreement (**NDA**) in original.
20. The Bidder shall provide integrity certificate stating that the solution supplied is **free from bugs, vulnerabilities, malwares and any covert channels in the code.**
21. Bidder should submit document mentioning **methodology of Strategy to identify various functional modules, tools deployed, business operational environment, execution setup, timelines and acceptance** criteria.

22. Bidder should be able to **calculate the effort needed to spend on auditing each requirement**, based on the requirement's level of business risk and available resources.

23. The bidder should also **take care of the entire defect life cycle from initial problem detection through fixing the defect and verifying the fix**. Therefore, no defect is overlooked or closed before it has been addressed.

24. Bidder shall provide **graphs and reports that will help analyze application readiness at any point in the process**. Provide graphs and reports using information about requirements coverage, planning progress, run schedules or defect statistics. Bank can make informed decisions on whether an application is ready to go live.

25. Bidder needs to prepare **strategy document listing the resources** to be deployed, execution methodology, reporting methodology, documentation deliverable.

26. The bidder is expected to use **best in class industry proven safeguards that prevents the misuse of information and appropriately protect the confidentiality, integrity and availability of information systems**. Follow industry standards during the whole SDLC Process.

27. Bidder should sign the Service Level Agreement (SLA) based services and SLA tracking system for maintaining operational workflow.

28. The Bidder shall also ensure that **the software does not and shall not contain any computer code or any other procedures**, routines or mechanisms to:

a. **Disrupt, disable, harm or impair** in any way the software or other applications installed on the system or interacts with orderly operation based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or other numeral (sometimes referred to as "time bombs", "time locks", or "drop dead" devices).

b. **Cause the software to damage or corrupt any of the Banks' or its clients' data, storage media, programs, equipment or communications, or otherwise** interfere with the Banks operations, or

c. **Permit the Bidder and/or its personnel and/or its licensors and/or any other third party, to access the software or any other software** or Banks computer systems to cause such disruption, disablement, harm, impairment, damage or corruption (sometimes referred to as "traps", "access codes" or "trap door" devices).

The scope of work shared above is only indicative and non-exhaustive. The bank and successful bidder will prepare an exhaustive list of work to be provided as a part of this proposed solution.

1.11 Training

Comprehensive training covering all aspects of Audit Management Solution (AMS), including all Functional and Technical aspects to be provided to Bank's all the identified staff. The tentative number of persons to be trained will be a maximum of **20** and they may be split into batches for training as per Bank's requirement. The TCO will include technical training, super user training, Log analysis & Monitoring and training materials (**both soft copy and hard copy**). The same should also be incorporated in the training manual/document. The training for the first batch should be completed before go-live date and for the remaining batches Bank will decide the schedule after confirming with the bidder. The bidder should provide the same without any extra cost.

1.12 Locations for work

Location for work will be Head Office, Regional Offices, Credit Processing Centers, Corporate Business Office, Project Monitoring Office and 823 Branches of Kerala Bank.

1.13 Timeline for Go-Live

Bank is expecting to Go-Live with the proposed Audit Solution, Implementation, Data Integration, Onsite & Offsite monitoring within **08 weeks from the date of issuing Letter of Intent / purchase order** to the selected vendor.

1.14 Attendance Report for Inspecting Officers

Attendance report for the Inspecting Officers posted in HEAD OFFICE should be available to Inspecting Officers.

1.15 Interface and Integration Requirements

1. The **Bidder** has to customize, implement, train and rollout the interfaces necessary for the functioning of the solution.
2. The Bidder is required to design, develop and maintain interfaces between the proposed Solution with the **applications and systems** mentioned below but not limited to:
 - **Core** Banking System
 - **LOS** (Loan Originating System)
 - **EWS** (Early Warning System)
 - Any other System as per Bank's requirement

1.16 Disaster Recovery Mechanism

The Bidder is expected to develop a disaster recovery plan for restoration of the system in the event of any disaster or major incident. **The Disaster recovery plan will be first tested prior to go- live to verify DR readiness** and then on every subsequent DR Drill conducted by Bank. The Bidder shall support during the DR drill and period will be decided by bank.

1.17 Implementation Methodology

The Bidder should follow a suitable methodology for delivering the requirements of the RFP for the entire Contract period. Accordingly, the Bidder should factor for necessary effort and team deployment. The methodology should clearly lay out the overall steps from initiation to closure of this engagement. The methodology should address all stages including development, customization, and hardware/software installation/configuration services. Each step should detail the input, process and output. The Bidder should further provide the deliverables and sign off process for each of the deliverables at various stages.

1.18 Functional Gap Specification Study

1. The Bidder is to suggest a work-around and replacement of customizations with standard functionality. The Bidder is expected to assist the Bank in aligning the business requirements with the application so as to enable centralization of desired business process, eliminate redundant and duplicate processes, increase operational efficiency and improve customer service. Bidder is expected to prepare detailed documentation, presentation, workflows for the business processes.
2. The Bank will identify functional heads for each process, which would be responsible for the review, comments and sign-off of the Implementation and Customization of Audit Software for Onsite and Offsite Monitoring.
3. The Implementation and Customization of Audit Software for Onsite and Offsite Monitoring software will be deemed completed when signed-off from the Bank.

1.19 Customization

1. The Bidder is expected to undertake a **detailed assessment of current system and procedures** for the Solution. The Bidder is expected to document the current state assessment and get the same reviewed and approved by the bank. The Bidder is also expected to identify the current state gaps between the procedures and practices followed by the Bank and requirements as per scope of this RFP being implemented and get the same reviewed and approved by the Bank.
2. The Bidder needs to provide **all existing management, statutory and regulatory reports as required by the regulatory authorities/institutions**. The Bank will not pay any additional customization costs either for gaps observed and/or gaps observed for existing management, statutory or regulatory reports as required by the Bank.
3. The Bidder is expected to provide a resolution to all gaps observed during Functional Requirement, Product Demonstration, Current Systems Study, Training, User Acceptance Testing (UAT), Business Process Definition (BPD) and subsequent roll out for all the proposed solutions. **The cost of customization should be included in the price bid.**
4. Over and above the Bank's existing reports, the Bidder must make **provision for configuration/customization/development and delivery of additional reports/MIS** from the Solution. Bank at its discretion may avail the development of any additional reports/MIS. The Bank will pay the proportionate amount on a pro-rata basis to the Bidder based on the number of reports delivered; post the satisfactory acceptance of the reports by the Bank.

1.20 Gap Identification and Resolution

1. The Bidder will provide the Bank with the **gap identification report** along with the necessary solutions to overcome the gaps and the time frames.
2. The Bidder will **ensure that all gaps identified** at the time of system testing will be immediately resolved.

3. The Bidder will ensure that **gaps pointed out by the audit and inspection teams, statutory and regulatory bodies, or any other third-party agency** engaged by the Bank will be immediately resolved.
4. The Bidder **shall resolve gaps by proposing a suitable work around or customizing the proposed solution by way of modifications/enhancements**, as necessary, to the proposed software solution.
5. The Bidder shall provide all **statutory, regulatory and ad hoc reports as required by the Bank** in the desired format during the initial phase of customization process
6. The Bidder shall **provide for all subsequent changes to reports as suggested by the statutory and regulatory bodies from time to time immediately to the Bank at no additional cost to the Bank** during the Contract period.
7. The Bidder will give **adequate time to the Bank for reviewing the gap report**.
8. The Bidder will incorporate **all the suggestions made by the Bank to the gap report**.
9. The Bidder will ensure that **they have the necessary infrastructure and people in place to resolve all the gaps within the time lines agreed**, for the implementation and roll out.
10. The Bidder is expected to **document all gaps observed by the Bank at various stages of implementation including their solution and monitor and track the status** of the same throughout the implementation.

1.21 UAT

For the implementation phase, all the testing, regression testing should be completed as per respective phased implementation. It will be the Bidder's responsibility to create the testing environment for the Bank's employees to do the testing and the Bidder will be required to assist the Bank in the entire testing phase.

1.22 Infrastructure (Hardware/Network)

The Bidder must include all hardware and network infrastructure components necessary to implement and maintain the solution for the full contract period, with details provided in the Technical Proposal.

Kerala Bank may provision these components through its DC/DR facilities or an alternate environment; otherwise, the Bidder shall provision them via a Meity-empannelled cloud solution.

1.23 Audit

All actions and activities performed within the system should have a **full audit trail** that not only simplifies troubleshooting and problem resolution but also provides an audit document to pinpoint accountability. The application architecture should also provide for easy drill down and scale up of information. Business logic should be available and verifiable "as of" a particular point in time to support comprehensive auditing requirements.

There should also be proper audit trail of addition, deletion, modification, activation, deactivation etc. of users and their system. In addition, there should also be proper audit trail of addition, deletion, modification,

at the record level showing the changes, users, dates and time stamp.

The system should be enabled to generate a detailed audit trail on a daily basis for the following minimum features:

- A. Attempted unauthorized logins
- B. Time of login and logout
- C. Change of passwords
- D. Change of parameters
- E. The audit trail should be at a granular level, and track the user across each activity
- F. All transactions should be time stamped with user ID along with details of modification, if any
- G. Details of databases accessed and modified by the users should be made available through the system
- H. The system should be enabled to store and track all system events, including corrections and cancellations by multiple criteria
- I. The system should maintain an error log in case of missing and/or erroneous data The bidder should also help to integrate proposed solutions with SIEM

1.24 Procedures in place to periodically test the backed-up data

The proposed solution should have necessary capacity, systems and procedures in place to periodically test **the backed-up data**, application pertaining to products to ensure recovery without loss of data or audit-trails. The proposed solution should have Data storage, security and privacy protection as per extant laws/ instructions.

1.25 Installation on existing or new setup

The successful Bidder should take care of all aspects of installation on existing or new setup, De- Installation, Configuration, Re-configuration, enhancements, updates, version upgrades, problem analysis, on-site, as well as off-site support to ensure smooth operations during and post implementation on perpetual basis.

1.26 Upgrade the proposed solution

The selected Bidder should upgrade the proposed solution if the same goes out of support or there is a need for up gradation for compliance to regulatory guidelines during the contract period without any additional cost to the Bank.

1.27 No unwarranted, illegal, and fraudulent misuse of data

The Bidder to ensure no unwarranted, illegal, and fraudulent misuse of data, shared by the Bank and Bidder to categorically indemnify the Bank against any losses that the Bank may suffer on account of any such fraudulent and illegal act by the Company or its employees.

1.28 Support for the present and future proposed interfaces

The scope of the Services, Maintenance and support is to be provided for the entire contract period as stipulated for the project along with maintenance and support of the present and future proposed interfaces to The Kerala State Co-operative Bank Ltd (Kerala Bank)

1.29 Support applicable as and when released by the OEMs

The selected Bidder has to provide support and applicable patches as and when released by the OEMs

connected with the proposed solution during warranty and thereafter during AMC period. Any observation raised by Regulators/Bank/Other Agencies from time to time should be rectified and fixed by the Bidder within one-week time after reporting without any additional cost. All patch updates and patch management of proposed solution modules has to be deployed by the selected Bidder after obtaining approval from The Kerala State Co-operative Bank Ltd (Kerala Bank)

1.30 Maintenance Support

The Bidder must provide uninterrupted availability of the system and ensure that the problem is resolved within the time schedule as prescribed in the Service Level agreement (SLA). The support includes, inter alia, maintenance, patch management, upgrades and troubleshooting, audit closures etc.

1.31 Facility Management

The Bidder has to provide **onsite one (1)** resource for facility management services **at Head Office** of the Bank for the period commencing from date of execution of Purchase order by both parties **till twelve months from the date of Go-Live** (preparation / foundation period) for integration, implementation, support, sustenance phases etc. The Bank presumes the cost of onsite resource will be provided in the commercial bid.

In case the above resources need to be replaced, the Bidder will use all reasonable endeavors to replace such individual(s) promptly by other sufficiently skilled, qualified, and experienced person(s) at no extra cost to the Bank. Bidder shall be solely responsible for acts and omissions of the said resource. In event of any loss, of whatsoever nature, is caused to the Bank due to acts and omission of the said resource, the bidder shall compensate the Bank to the extent of such loss.

Considering the extensive nature of the assignment and the envisaged relationship with the Bidder, any service which forms a part of facilities management that is not explicitly mentioned in this RFP as exclusion would form part of this RFP and the Bidder is expected to provide the same at no additional costs to the Bank. The Bidder has to envisage all necessary services to be provided and ensure the same is delivered to the Bank. The Bank will not accept any plea of the Bidder at a later date for omission of critical services on the pretext that the same was not explicitly mentioned in the RFP.

1.32 Artificial Intelligence Compliance Requirements

This outlines mandatory AI compliance requirements for vendors providing AI-enabled solutions to the Bank, based on RBI's Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI).

1. Guiding Principles

- Trust is the foundation of all AI engagements.
- People First – Ensure human oversight for critical decisions.
- Fairness and Equity – AI outcomes must be unbiased and inclusive.
- Accountability – Vendors remain responsible for AI-driven decisions.
- Understandable by Design – AI systems must be explainable.
- Safety, Resilience, and Sustainability – Secure and robust AI systems.

2. Governance and Risk Management

- Board-approved AI policy for vendor engagements.
- AI risk classification (Low, Medium, High) for proposed solutions.
- Lifecycle governance: documentation, validation, monitoring, and decommissioning.
- Mandatory explainability and transparency of AI models.

3. Data Privacy and Security

- Compliance with DPDP Act and RBI norms.
- Bias detection and mitigation in AI models.
- Data lineage and traceability for AI training datasets.
- Restrict use of customer data unless explicitly approved.

4. AI Risk Mitigation

- Red Teaming for AI models before deployment and periodically.
- AI-specific BCP/DR plans for model failures.
- Incident reporting within 24 hours for AI-related failures.

5. Procurement and Evaluation

- Disclosure if solution uses AI/ML, with model type and explainability features.
- Provide bias audit reports and interpretation tools.
- Participation in AI Innovation Sandbox for testing.

6. Monitoring and Audit

- Periodic AI audits covering input data quality, fairness, and robustness.
- Maintain AI inventory for regulatory reporting.

7. Consumer Protection

- Inform customers when interacting with AI systems.
- Provide human override option for AI-driven decisions.

8. Contractual Clauses

- Include AI-specific obligations in SLAs (accuracy, fairness, explainability).
- Vendor liability for AI-driven harm (bias, incorrect decisions).
- Commitment to continuous model monitoring and updates.

The proposed Audit Management Software shall incorporate advanced Artificial Intelligence (AI) capabilities utilizing a Model Context Protocol (MCP) or equivalent framework, along with an orchestration layer in agentic AI, to analyze multiple audit reports and identify common, correlated, and recurring observations across diverse audit engagements. The solution shall be capable of ingesting structured and unstructured audit findings from multiple reports, standardizing varied expressions of similar issues, and applying semantic analysis to detect patterns, similarities, and root causes. The agentic AI orchestration layer shall coordinate multiple AI agents to perform tasks such as data normalization, contextual interpretation, cross-report comparison, and risk aggregation. Based on this analysis, the system shall automatically generate a

consolidated **Risk Profile**, highlighting critical observations, systemic control weaknesses, and emerging risk themes across audits. The AI engine shall support contextual learning, continuous improvement, and explainable outputs, enabling auditors and management to prioritize high-risk areas, track recurring issues, and support informed decision-making for risk mitigation and governance.

1.33 Compliance to Digital Personal Data Protection (DPDP) Act 2023

The proposed Audit Module solution and the successful bidder shall strictly comply with the provisions of the Digital Personal Data Protection Act, 2023 and all rules, regulations, notifications, and amendments issued thereunder. The solution must ensure lawful processing of digital personal data, implementation of appropriate technical and organizational security safeguards, data minimization, purpose limitation, storage limitation, access controls, encryption, audit trails, breach detection and reporting mechanisms, and support for data principal rights including access, correction, and erasure. The bidder shall act only on documented instructions of the Bank, maintain confidentiality of personal data, ensure data localization as applicable, and promptly notify the Bank of any personal data breach in accordance with statutory timelines. The bidder shall also facilitate audits, inspections, and compliance assessments by the Bank or regulatory authorities and shall remain fully responsible for ensuring end-to-end compliance throughout the contract period.

1.34 Software Bill of Materials (SBOM)

The bidder shall provide a complete and up-to-date Software Bill of Materials (SBOM) for the proposed Audit Module solution at the time of submission of technical proposal and upon every major release or update during the contract period. The SBOM shall include a comprehensive inventory of all software components, libraries, frameworks, modules, and dependencies (including open-source and third-party components), along with their version numbers, licensing details, and known vulnerabilities (if any). The SBOM shall be provided in a machine-readable format and must enable the Bank to assess supply chain risks, security vulnerabilities, and license compliance.

SECTION : II GENERAL CONDITIONS OF CONTRACT AND SERVICE LEVELS AGREEMENT

2.1 General

- **Quality:** Material/solution not conforming to given specifications will be rejected & it will be replaced by the vendor, free of cost. The material/solution must be as per the detailed specifications listed out in RFP document and shall be as per standard engineering practice, relevant IS/ Imitational code of practice, and shall be as per the Specifications as mentioned in RFP Document.
- **Statutory Laws:** Vendor shall abide by all applicable rules and regulations regarding taxes, duties, labor etc., which are in force and from time to time enforced by the Government of India, also registration, labor laws, payments, ESIC, PF, insurance etc. Vendor shall coordinate for all these matters with concerned authorities directly.
- **Confidential Information:** All information exchanged between the parties will be confidential. If the implementation project requires disclosure of, or receipt of, confidential information, such disclosure or receipt will be made with mutual agreement and may be with a separately executed MoU / Non-Disclosure agreement with Vendor by the Bank.
- **Extra Deviated Items:** Any extra item like variation in quantity, deviated item should be executed only after getting the appropriate approvals with written confirmation, from the bank. At the time of submitting the invoice, all the documentary evidence of appropriate approvals for Extra / deviated Items / Variation in Quantities should be attached. Payments will not be made without scrutiny of aforesaid approvals.
- **Force Majeure:** Bank shall not be responsible for delays or non-performance of any or all obligations, contained in this RFP or agreement thereafter, caused by war, revolution, insurrection, civil commotion, riots, mobilizations, strikes, blockade, acts of God, Plague, epidemics or pandemics, fire, flood, obstructions of navigation by ice of Port of dispatch, acts of government or public enemy or any other event beyond the control of the bank, which directly, materially and adversely affect the performance of any or all such obligations. However, the bidder shall continue to perform its obligations as contained in this RFP and agreement thereafter.
- **Arbitration:** The Bank and the Bidder shall make every effort to resolve amicably, by direct negotiation between the respective Designated Officials of the Bank and the Bidder, any disagreement or dispute arising between them under or in connection with the RFP and or contract thereafter.

If the designated official of the Bank and the Bidder are unable to resolve the dispute within -30- days from the commencement of such informal negotiations, they shall immediately escalate the dispute to their Senior Authorized Person.

If within -30- days from the commencement of such negotiations between the Senior Authorized Person designated by the Bidder and Bank, are unable to resolve their dispute amicably, in such case the dispute shall be settled finally by arbitration and in accordance with the provisions of the Arbitration and Conciliation Act, 1996 or any statutory modification or re-enactment thereof. The right to appoint arbitrator shall lie with the bank only. Cost of arbitration shall be borne equally by both parties.

- **Jurisdiction:** The Jurisdiction for all disputes will be in the city of Ernakulam.
- **Safety:** All the safety codes and the preventive measure for this type of work shall be strictly followed. In case of any mishap which causes injury, disability or death of any personnel and staff either on site or offsite during or after the duration of the project due to negligence of the staff of the vendor, shall be sole responsibility of vendor, this shall not be responsibility of Bank in any case. No Claims in this regard shall be paid by Bank.
- **Integrity:** The prospective Vendors / Bidders/Contractors and the Bank, commit that the persons / officials of both the parties shall not resort to any corrupt practices during or after the tendering process and contract execution.

2.2 Term and Extension of the Contract

The term of this Contract will commence from the date of signing of contract/agreement and will be **valid for a period of five (5) years**. The contract is extendable further for two (2) years solely at the option of Bank.

The Bank shall reserve the sole right to grant any extension to the term above mentioned and shall notify in writing to the Bidder, at least 6 months before the expiration of the Term here of, whether it will grant the Bidder an extension of the Term. The decision to grant or refuse the extension shall be at the Bank's discretion.

During extended period of two years if deemed appropriate the term and conditions for SLA, penalty and Prices for On-premise services, AMC & Manpower shall remain same as given for 5th Year.

Where the Bank is of the view that no further extension of the term be granted to the Bidder, the Bank shall notify the Bidder of its decision at least 6 (six) months prior to the expiry of the Term. Upon receipt of such notice, the Bidder shall continue to perform all its obligations hereunder, until such reasonable time beyond the Term of the Contract within which the Bank shall either appoint an alternative service provider or create its own infrastructure to operate such Services as are provided under this RFP. In such scenario, the terms and conditions for SLA, penalty and Prices for On-premise services, AMC & Manpower shall remain same as given for 5th Year.

2.3 Warranty

- a) The warranty of 12 Months shall start from the date of UAT Sign-Off. Any defects / bugs noticed in the migrated/implemented applications shall be reworked and / or replaced by the Bidder / Vendor with defect-free components free-of-cost.
- b) Bidder / Vendor should provide software patches / upgrades towards complying with all the statutory and any other requirements from the Bank as specified from time to time during the Contract period, free of cost. The warranty period would start after live implementation*

(*Live implementation means that after user acceptance and audit clearance the complete System is ported on the production environment (Go Live) and after issuance of Acceptance Certificate by the Bank).

- c) Bidder should setup **one centralized L2 Support at Bank Site** till the completion of warranty period as mentioned above. The Bank has a right to interview and reject resources deployed by the Bidder.

2.4 Prices

Prices quoted must be firm and shall not be subject to any upward revision on any account whatsoever throughout the period of contract. However, if there is any increase/decrease in taxes due to any reason whatsoever, after Notification of Award, the same shall be passed on to The Kerala State Co-operative Bank Ltd (Kerala Bank) In any circumstances no other additional cost shall be payable by the Bank on account of any software / tools used by the Service Provider for rendering the services as required in the Tender. The bidder should make his own arrangement for providing such software / tools used at his own cost. The responsibility to ensure that only legal, authorized, licensed versions of software / tools provided by the bidder and used by its employees are used for extending the required services, lies solely with the bidder.

The Bank in no way be a part of any litigation arising out of using unauthorized software / tool used by the bidder/service provider.

2.5 Payment Terms and Schedule

The payment would be disbursed on completion of each milestone as mentioned in table below. The milestone-based pay-out percentages are defined in the table below:

- 20% on successful POC
- 20% on successful UAT
- 10% on successful integration of proposed solution with Finacle 10.x
- 35% on successful GO-LIVE of the proposed solution
- 15% as Security Deposit

For any other cost as submitted by the bidder, the payment terms will be decided at the time of signing of agreement.

The Vendor's request(s) for payment shall be made to "The Kerala State Co-operative Bank Ltd (Kerala Bank)" in writing accompanied by Invoice and Service Level Requirements compliance reports for which payment is being claimed.

All the payments to the Vendor shall be subject to the report of satisfactory accomplishment of the concerned task. Penalties, if any, on account of liquidated damages and non-compliance of Service Level Requirements, shall be deducted from the invoice value.

Payments will be released only on satisfactory acceptance of the deliverables for each Task as per the particulars mentioned in the commercial bid.

All Payments shall be made in Indian Rupees Only and shall be released by the Bank against the invoices raised by bidder within 30 calendar days given all the relevant documents are submitted timely and are complete in all reference.

Note:

- Payments should be subject to deductions of any amount for which the Bidder is liable under the RFP conditions. Further, all payments shall be made subject to deduction of TDS (Tax deduction at Source) as per the applicable Income-Tax Act.
- No advance payment will be made.

2.6 Service Level Agreement & Targets

The selected vendor has to sign a detailed SLA before the issuance of Purchase Order. The SLA will be prepared jointly by the Bank & the selected vendor and will be based on

- The scope of the RFP and any amendment done in the RFP before submission of the bid.
- The solution offered by the vendor in response to the bid.
- The SLA will be binding on the vendor for the entire period of term of contract.
- The Penalty clause shall be defined in SLA.

2.7 Quality & Cost Based Selection (QCBS)

Bids are evaluated using QCBS –Quality and Cost Based evaluation method where Quality will be having highest priority and Cost will be the next priority. 70:30 weightage for Technical and Financial Score will be used to arrive the Combined Technical and Financial Score (CTFS)

2.8 Integrity Pact

The bidder has to enter into an Integrity Pact with the Bank to the effect that they will not resort to any corrupt practice in any aspect/stage of the contract. Only those bidders who enter such a contract with the bank will be considered for participation in the tender.

2.9 Liquidated Damages (LD)

- If the selected Bidder fails to complete the due performance of the contract in accordance with the specifications and conditions agreed during the agreement, the Bank reserves the right to recover LD @ 5% of the total Charges per week of the yearly order value, subject to a maximum of 20 % of total charges as liquidated damage for non-performance or delayed performance. This would be in addition to penalty

- Liquidated Damage is not applicable for delay due to reasons attributable to the Bank and Force Majeure. However, it is the responsibility of the Bidder to prove that the delay is attributable to the Bank or Force Majeure.

2.10 Eligibility Criteria

- Registered startup under Kerala Startup Mission KSUM
- Demonstrated experience in fintech/Regtech, API integration, or AI/ML
- Prior PoC, pilot, or hackathon experience in financial services preferred.
- If the proposed solution has not yet been implemented, a POC with the Bank is required.
- Team with expertise in:
 - API aggregation and orchestration AI/ML and NLP
 - Cybersecurity and compliance
 - UX design for rural/low-literacy users

FUNCTIONAL REQUIREMENTS

1. ANNEXURE-1_BRANCH INSPECTION RISK RATING PERFORMA (Attached)
2. ANNEXURE-2_PACS OR OTHER SOCIETIES INSPECTION PERFORMA (Attached)
3. ANNEXURE-3_INSPECTION BY REGIONAL OPERATIONS MANAGER PROFORMA (Attached)

ANNEXURES

Please Click Here To Download [ANNEXURE-1 BRANCH RISK RATING PERFORMA final 02-06-2026.xlsx](#)

Please Click Here To Download [ANNEXURE-2 PACS OR OTHER SOCS INSPN PERFORMA UPDTS 4-6-25.xlsx](#)

Please Click Here To Download [ANNEXURE-3 INSPECTION By ROMs.xlsx](#)