Intelligent Alert automation Solution (IAS)

Issued by: Kerala State Cooperative Bank (KSCB)

In collaboration with: Kerala Startup Mission (KSUM)

Reference No: [KBIT/PMU/Intelligent Alert Solution/082/2025-26]

Table of contents

1. Introduction

The Kerala State Cooperative Bank (KSCB), the apex cooperative bank of Kerala, invites proposals from eligible startups registered under Kerala Startup Mission (KSUM) for the phased design, development, implementation, and support of a future-ready an Intelligent Alert automation Solution (IAS) to automate the end-to-end lifecycle of compliance AML alerts in the bank.

The solution should integrate seamlessly with AML systems, applies AI-driven classification under PMLA guidelines, and provides branch-level visibility for suspicious transactions. The solution ensures timely communication with regulatory bodies (FIU), supports closure workflows, and reduces manual intervention through adaptive learning. Its goal is to strengthen compliance, minimize operational risk, and enhance efficiency in monitoring suspicious activities.

The system must be scalable, API-first and compliant with RBI, PMLA, and DPDP Act. It must integrate with national and Kerala state APIs, support refinancing workflows, and embed orchestration and AI layers for automation and inclusivity.

2. Objectives

- Implement an AI-driven alert automation solution to strengthen compliance monitoring under PMLA.
- Integrate seamlessly with AML systems to ingest and process alerts in real time.
- Provide branch-level dashboards for visibility into suspicious transactions.
- Automate communication with FIU through secure email and system integration.
- Ensure timely closure of alerts with complete audit trails.

3. Scope of Work

3.1 Functional Scope

- Seamless interoperability with existing Anti-Money Laundering platforms for unified monitoring.
- Automated detection and categorization of suspicious transactions under PMLA guidelines.

- Granular dashboards and reports enabling local branches to track and act on flagged activities.
- Real-time, secure reporting and alerting to FIU and other mandated authorities.
- Structured case management processes to ensure timely resolution of suspicious activity reports.

3.2 Technical Scope

- API-first, microservices-based architecture
- Integrations with CBS, DMS, AML, Bank's allied solutions
- MCP orchestration layer
- Agentic AI and Generative AI modules
- Secure data storage, encryption, and audit logging

3.3 Compliance Scope

- Must comply with RBI, FREE-AI Framework, PMLA, and FIU guidelines.
- PMLA: AML/KYC, CTR/STR reporting
- DPDP Act: Consent, Minimization, Erasure, Portability
- ISO 27001 and CERT-In cybersecurity controls

4. Deliverables

- **Integration with AML alert systems**: Real-time ingestion and processing of alerts.
- **AI-based segregation engine**: Classification of alerts into suspicious and non-suspicious categories under PMLA.
- **Branch-level dashboard**: Interactive dashboards for branch compliance officers to monitor suspicious transactions.
- **FIU and email integration**: Automated reporting and communication with FIU and internal stakeholders.
- **Alert closure workflows**: AI-assisted resolution paths with SLA tracking and documentation.
- **Audit trail and compliance reporting**: End-to-end logging of alert lifecycle for regulatory audits.

Additional:

- Technical documentation

- User manuals and training materials
- SLA-backed support and maintenance plan

5. 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

6. Evaluation Criteria (QCBS 70:30)

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.

STAGE 1: TECHNICAL BIDS EVALUATION [e.g.]

Bidder details	Technical Marks Obtained	Technical Score (TS*)
Bidder1	92 (T1)	(92/92) * 100 = 100
Bidder2	85	(85 / 92) * 100 = 92.39
Bidder3	55	Not applicable
Bidder4	75	(75 / 92) * 100 = 81.52

*Technical score is calculated as TS = (Technical Mark obtained by the bidder / Highest Technical Mark amongst bidders) * 100

The bidders who score 70 marks or above in the technical evaluation will be qualified for Financial Bid evaluation.

STAGE 2: FINAL BID EVALUATION [e.g.]

Bidder details	Financial Bid Amount discovered

Bidder1	1,30,000
Bidder2	1,20,000
Bidder4	1,00,000

Note: The associated infrastructure costs will also be added for the calculation of the Total Project Cost.

STAGE 3: CONVERSION OF FINANCIAL BID AMOUNT TO SCORE [eg]

Bidder Details	Financial Bid Amount discovered	Financial Score (LFB/F*100)
Bidder1	1,30,000	(100000/130000)*100=76.92
Bidder2	1,20,000	(100000/120000)*100= 83.33
Bidder4	1,00,000 (L1)	(100000/100000)*100 =100

LFB = Lowest Financial Bid from Financial Bid, F = Quoted Amount in Financial Bid

Consolidated Technical & Financial Score (e.g.)

Bidder Details	Technical Score	Financial Score
Bidder 1	100	76.92
Bidder 2	92.39	83.33
Bidder 4	81.52	100

STAGE 4: COMBINED TECHNICAL AND FINANCIAL SCORE (CTFS)

70:30 weightage for Technical and Financial Score will be used to arrive the Combined Technical and Financial Score (CTFS)

Bidder Details	Applying weights for the Technical Score & Financial Score	CTFS	Rank of the Bidder
Bidder1	100*(70/100) + 76.92*(30/100)= 93.076	93.076	1
Bidder2	92.39*(70/100) + 83.33*(30/100) = 89.672	89.672	2
Bidder4	81.52*(70/100) + 100*(30/100)= 87.064	87.064	3

7. Implementation Timeline

Sl.No	Milestone	Timeline – days
1	Issuance of Purchase Order	T
2	Signing of the agreement, Finalise and signing of implementation Project plan	
3	Finalisation of SRS and integration requirements	
4	Successful completion of Customization, integration Configuration and pre-delivery testing	
5	Delivery of Functional and non-functional test results Successful completion of UAT. Delivery of Training and Training materials	
7	Go-live preparation Finalise support process.	
8	Go-live	T+45 days

8. Proposal Submission Guidelines

- Submit technical and financial proposals separately when asked for by Kerala Startup Mission.

9. Terms & Conditions

- KSCB reserves the right to accept/reject proposals
- Data privacy and DPDP compliance are mandatory
- SLAs must define uptime, response times, and support levels
- Selected vendor must sign a Non-Disclosure Agreement (NDA)

10. Projected Branch / Office Expansion

Current Scenario	**No of Branches & Offices**
	850

The solution proposed by the bidder should be scalable to handle the load for projections. The resource (CPU/ memory / utilization) at given projection should not go beyond 70% there should not be any single point of failure in the entire software solution. The entire solution should be configured in high availability mode both at DC and DR with inbuilt redundancy.

So, the bidder has to calculate the data growth based on the standard assumption in the industry. This is applicable for all other services which are presently in use and that might get included in future.

11. 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-empanelled cloud solution.

12. Facility Management Services

The FM support - with minimum One L2 resources should be deployed at Bank's premises, for supporting the solution primarily for 10 hours (viz. 9 am to 7 pm) or as decided by the Bank. However in case of exigency the Bidder shall provide and maintain requisite skilled resources for extended hours as required.

13. Integrity Pact

The Integrity Pact shall be executed by the Bidder, duly stamped and signed on each page, and witnessed by two individuals.

14. Escrow / Similar arrangements

The bidder shall be required to establish and execute an Escrow or equivalent arrangement to ensure that the complete source code, along with all related customization details, is securely deposited with a designated third-party location.

15.Confidentiality

The bidder, by participating in the bidding process, shall regard all document details as strictly confidential. The bidder must undertake that they shall hold in trust any information received by them under the contract /agreement, and the strictest of confidence shall be maintained in respect of such information.

16. Performance & security audit

This is an important step that ensures accuracy, availability and security of the data. Bank will identify a suitable audit firm to conduct performance & security audit in compliance with the norms set by regulator for which the selected bidder should furnish all necessary information and support in the form prescribed by the audit firm. The selected bidder has to rectify all the performance and security audit comments to the satisfaction of the Bank without any additional cost.

17. Penalty

The successful bidder must strictly adhere to the delivery periods and timelines in the implementation schedule. Failure to meet these delivery dates, unless it is due to reasons entirely attributable to the Bank, may constitute a material breach of the bidder's performance. As a deterrent for delays during implementation, Bank may levy penalties for delays attributable to the successful bidder.

18. Contract Period

5 years.

19. Annexures

Annexure I - Functional requirements

The form has to be filled in all respects. If any raw is left blank it will be categorized as "Not Possible" for evaluation purpose.

Sl#	Description	Readily Available (RA)	Customisable (CA)	Not Available (NA)
I	**General requirements**			
1	The solution should be device independent and work seamlessly on devices such as desktops, laptops, mobiles, tablets etc.			
2	The solution should be available in multiple languages i.e. should have Unicode support.			
3	The solution should be fully web- based with preferably no client component installation required on the user's work station.			
4	The solution should be platform Independent. It should support commonly used open source and proprietary platforms (OS, DB, Web Server, App Server, monitoring platforms etc)			
5	The solution should be secure with complete access and role management features.			
6	The solution must not, by its own architecture or design, impose any practical limit on the number of files/ documents that can be created/ handled at any point			
7	The solution should be compatible with technologies and communication platform running within in KSCB.			
8	The system must offer full application security and information on all security events must be recorded on an audit trail.			
9	The solution should be able to be accessed remotely, via VPN or Internet			
Ii	**Core Functionalities**			
10	Real-time AML integration: Seamless ingestion of alerts from existing AML solution			
11	AI-driven classification: Automated segregation of suspicious vs. non-suspicious alerts under PMLA guidelines.			
12	HO/Branch-level dashboards: Localized visibility for branch compliance officers to monitor and act.			
13	Regulatory reporting integration: Automated communication with FIU via secure channels.			
14	Alert closure workflows: AI-assisted resolution paths with SLA tracking.			
15	Adaptive learning models: Continuous improvement based on feedback from closed alerts.			

16	Escalation management: Automatic routing of high-risk alerts to compliance heads.			
17	Audit trail logging: End-to-end lifecycle tracking for regulatory audits.			
18	Multi-channel notifications: Email, SMS, WhatsApp and dashboard alerts for timely action.			
19	Role-based access control: Restricting sensitive alerts to authorized personnel only.			
Iii	**Advanced Functional Requirements**			
20	Case management system: Centralized repository for tracking alert investigations.			
21	Workflow customization: Configurable resolution paths based on risk category.			
22	Integrations:- Bank's ALM, CBS, CRM,LOS etc -Cross-platform data sharing for contextual analysis.			
23	Regulatory compliance templates: Predefined reporting formats aligned with FIU/PMLA.			
24	Automated SLA monitoring: Alerts for breaches in resolution timelines.			
25	Risk scoring engine: Assigning severity scores to alerts for prioritization.			
26	Data enrichment: Pulling customer and transaction data for contextual analysis.			
27	Duplicate alert suppression: Intelligent merging of similar alerts to reduce redundancy.			
28	Cross-branch visibility: Compliance heads can view aggregated alerts across branches.			
29	Secure communication channels: Encrypted messaging for internal and external stakeholders.			
Iv	**Monitoring & Analytics Requirements**			
30	Performance dashboards: KPIs on alert volumes, closure rates, and false positives.			
31	Predictive analytics: Identifying emerging suspicious patterns proactively.			
32	Regulatory audit reports: On-demand generation of compliance reports.			
33	User activity monitoring: Tracking actions taken by compliance staff for accountability.			
34	System health monitoring: Real-time checks on integrations, workflows, and notifications.			
These are indicative requirements. Final functionalities must be implemented by the vendor as determined in the detailed system study.				

Annexure II – Technical requirements

The form has to be filled in all respects. If any raw is left blank it will be categorized as "Not Possible" for evaluation purpose.

Sl #	Description	Readily Available (RA)	Customisable (CA)	Not Availabl e (NA)
1	**High Availability architecture**: Solution must run in HA mode with minimum 99% uptime.			
2	**Disaster Recovery (DR) support**: Real-time replication to DR site with manual/automatic failover.			
3	**Scalability**: Ability to increase concurrent instances to keep CPU/memory utilization below 70%.			
4	**Multi-environment deployment**: Production, Pre-production, DR, UAT, and Training environments supported.			
5	**Platform independence**: Solution should be hardware/OS agnostic.			
6	**Lightweight application design**: Optimized for low-bandwidth branch access.			
7	**Database & OS clustering**: Native support for clustering to ensure resilience.			
8	**System health monitoring**: Continuous monitoring of application, database, and integration points.			
9	**Single Sign-On (SSO)**: Integration with Finacle CBS, ALM, AD, and IDAM solutions.			
10	**Encryption in transit**: AES/TLS-based encryption for CBS and external interfaces.			
11	**Data integrity assurance**: Hashing algorithms (SHA-2 or higher) for integrity checks.			
12	**Audit trail logging**: Comprehensive logs for all users, including admin actions.			
13	**Segregation of duties**: Multi-level admin roles (system, functional, branch-level).			
14	**Web application security**: Protection against XSS, SQL injection, broken authentication, etc.			
15	**Compliance with IT/Cyber Security policies**: Adherence to RBI, PMLA, and Bank's IT policy			
16	**Data localization & privacy compliance**: Must meet statutory norms for data residency.			
17	**Integrations**: Bi-directional data exchange facility with CBS, AML.			
18	**Middleware/API support**: REST, SOAP, JSON, XML, ISO 8583 formats supported.			

19	**Negative database interfacing**: Capability to connect with external fraud/blacklist databases.			
20	**STP mode integration**: Straight-through processing with minimal manual intervention.			
21	**FinTech integration**: Open APIs for third-party/FinTech collaboration (sync & async calls).			
22	**Messaging protocol support**: Standard protocols for interfacing with internal/external systems.			
23	**Store-and-forward mechanism**: Ensures continuity during communication breakdowns.			

Annexure III – Details of Proposed Network components

Serial Number	Item Description	Make & Model	Version/Specification	Capacity such as number of ports/connections	No of License/users	Warranty Period	Support Details	Any other information

Annexure IV – Details of Proposed Hardware Infrastructure

Serial Number	Make & Model	Processor Type & clock speed	Number of cores per server	Total Memory per server	Hard Disk type& capacity etc. per server	RAID Particulars per server	Operating System per server	Redundant Network bandwidth per server	Redundant Power Supply (RPS)	Number of Physical servers	Other particulars such as HBA	whether deployed in VM /shared	Function / purpose

Annexure VI - Declarations

- Eligibility Declaration
- Conflict of Interest Declaration
- NDA Acceptance
- Integrity Pact
- Details of Existing Installations