TECHNICAL REQUIREMENTS – ANTI-MONEY LAUNDERING SYSTEM

Notes on the Technical Requirements

The technical requirements define the system for Anti-Money Laundering System. The objective is to implement the system.

Table of Contents: Technical Requirements

1. ACRONYMS USED IN THE TECHNICAL REQUIREMENTS

Acronym Table

	Term	Explanation
1	API	An application programming interface It is a type of software interface, offering a service to other external systems or platforms
2	DBMS	Database Management System
3	AML	Anti-Money Laundering System
4	CDD	Customer Due Diligence
5	KYC	Know Your Customer
6	CRM	Customer Relationship Management
7	QA	Quality Assurance Test Requirements
8	SL	Sanction List

2. FUNCTIONAL, ARCHITECTURAL, PERFORMANCE AND GENERAL TECHNICAL REQUIREMENTS

2.1. Legal and Regulatory Requirements to be met by the AML

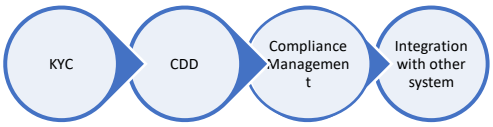
2.1.1. The System MUST comply with the following laws and regulations:

2.1.1.1. Kenya Data Protection Act 2019

2.1.1.2. Ethiopia Computer Crime Proclamation No. 958/2016

2.2. Business Function Requirements to be met by the Information System

The objective of the Anti-Money Laundering (AML) system implementation for the DRIVE (De-risking, Inclusion, and Value Enhancement) project, funded by the World Bank, is to establish a comprehensive and effective AML framework that promotes de-risking of the enterprise from money laundering and other illicit activities, ensures inclusion of pastoralists and farmers in the Horn of Africa, and enhances the overall value of financial transactions. The AML system aims to leverage advanced technologies and automation to streamline customer due diligence (CDD), transaction monitoring, and suspicious activity reporting, while adhering to relevant regulations and best practices. The system will also emphasize the identification and reporting of sanctioned individuals and entities, as well as monitoring financial transaction destinations that are under sanctions by the United States. By mitigating the risks associated with money laundering, including the detection of sanctioned parties and entities, the AML system will contribute to creating a safer and more inclusive financial environment for pastoralists and farmers in the Horn of Africa, fostering sustainable development and promoting integrity in financial transactions for the benefit of all stakeholders involved in the DRIVE project.



1. Know Your Customer (KYC) Systems: This system should verify the identity of our customers and maintain updated records of their transactions, in brief complete the first step of Customer Due Diligence. KYC systems will help prevent fraud and identity theft and assist in identifying potential money laundering activity.
    a. Clients' complete information submission as per template. Template should be customisable.
    b. Business owner receives notification of submission.

c. Business owner evaluates based on set criteria and determines if Enhanced CDD is required.
d. If not required, proceed to contract the business.
e. If required, perform CDD process.

2. Enhanced Customer Due Diligence (CDD): The system should be able to gather and verify information about customers and their business activities, including their identity, source of funds, and beneficial ownership.
    a. Business Owner collects additional data for due diligence. System should keep a checklist to be used in the data collection.
    b. Software should enable countercheck against any one of the world bank approved sanctions list, and the OFAC, UN, AU sanctions lists.
    c. Based on the outcome, contract or reject the transaction including working with the individual.
3. Compliance Management: This system should generate and maintain documentation of policies, procedures, and controls that are designed to prevent and detect financial crimes.
4. Integration with other systems: The system should be able to integrate with other internal and external systems, in order to obtain additional data and improve the accuracy of its analyses, as well as validation before any master data creation. More integrations would be an advantage.

2.3. Architectural Requirements to be met by the Anti-Money Laundering System

2.3.1. The System MUST be supplied and configured to implement the following architecture.

Component	Description
Data Sources	Internal and external databases, watchlists, and sanctions lists
Data Processing	Data ingestion, parsing, and normalization
Rules Engine	A set of rules and algorithms to detect and alert on suspicious activities and transactions
Workflow Engine	A set of workflows to process alerts and cases, including investigation, escalation, and reporting
User Interface	A web-based application for users to access the system's functionalities, including monitoring, investigation, and reporting
Reporting	A set of reports and dashboards to provide insights and metrics on AML activities, including transaction monitoring, investigations, and reporting
Security	A set of security measures to protect sensitive data and prevent unauthorized access, including encryption, authentication, authorization, and auditing
Infrastructure	A set of hardware and software components to support the system's functionalities, including servers, storage, networking, and cloud services

2.4. Systems Administration and Management Functions Required to be met by the Anti-Money Laundering System

Scalability: The AML system should be able to handle a large volume of data and transactions, as the project targets pastoralists and farmers in the Horn of Africa, requiring the system to be capable of processing a potentially high number of financial transactions.

Data Integration: The system should be able to integrate with various data sources, such as internal and external databases, watchlists, and sanctions lists, to ensure comprehensive screening and monitoring of customers, transactions, and destinations.

Real-time Monitoring: The AML system should provide real-time monitoring capabilities to detect and alert people to suspicious activities and transactions in a timely manner, enabling quick and effective response to potential money laundering activities.

Compliance with Regulations: The system should comply with relevant regulations, including those related to AML, sanctions, and data privacy, to ensure legal and regulatory compliance in the targeted regions, including the monitoring of financial transaction destinations under sanctions by the United States.

Security: The AML system should have robust security measures in place to protect sensitive financial data and prevent unauthorized access. This includes encryption of data, secure authentication and authorization mechanisms, and regular security audits and updates to address potential vulnerabilities.

System Integration: The system should be easily integrated with existing enterprise systems, such as customer relationship management (CRM) systems, transaction processing systems, and reporting systems, to ensure seamless data flow and efficient processing of AML activities.

Disaster Recovery: The system should have a disaster recovery plan in place, including regular data backups, redundant system architecture, and failover mechanisms, to ensure high availability and minimal downtime in case of system failures or disasters.

Testing and Documentation: The system should undergo comprehensive testing, including functional and security testing, with documented results and resolutions of identified issues. Proper documentation, including user manuals, system architecture, and system configuration details, should be maintained for reference and auditing purposes.

Training and Support: The system should provide training and support to users, including system administrators and compliance officers, to ensure proper understanding and utilization of the system's functionalities, as well as prompt support in case of issues or inquiries.

Audit and Reporting: The system should have **a** robust audit and reporting capabilities to track and document all activities and transactions processed by the system, including suspicious activity reports (SARs), to meet regulatory requirements and facilitate auditing and reporting to relevant stakeholders.

2.5. Performance Requirements of the Information System

Scalability: The AML system should be able to handle a large volume of data and transactions, as the project targets pastoralists and farmers in the Horn of Africa, requiring the system to be capable of processing a potentially high number of financial transactions.

Data Integration: The system should be able to integrate with various data sources, such as internal and external databases, watchlists, and sanctions lists, to ensure comprehensive screening and monitoring of customers, transactions, and destinations.

Real-time Monitoring: The AML system should provide real-time monitoring capabilities to detect and alert people to suspicious activities and transactions in a timely manner, enabling quick and effective response to potential money laundering activities.

Compliance with Regulations: The system should comply with relevant regulations, including those related to AML, sanctions, and data privacy, to ensure legal and regulatory compliance in the targeted regions, including the monitoring of financial transaction destinations under sanctions by the United States.

Security: The AML system should have robust security measures in place to protect sensitive financial data and prevent unauthorized access. This includes encryption of data, secure authentication and authorization mechanisms, and regular security audits and updates to address potential vulnerabilities.

System Integration: The system should be easily integrated with existing enterprise systems, such as customer relationship management (CRM) systems, transaction processing systems, and reporting systems, to ensure seamless data flow and efficient processing of AML activities.

Disaster Recovery: The system should have a disaster recovery plan in place, including regular data backups, redundant system architecture, and failover mechanisms, to ensure high availability and minimal downtime in case of system failures or disasters.

Testing and Documentation: The system should undergo comprehensive testing, including functional and security testing, with documented results and resolutions of identified issues. Proper documentation, including user manuals, system architecture, and system configuration details, should be maintained for reference and auditing purposes.

Training and Support: The system should provide training and support to users, including system administrators and compliance officers, to ensure proper understanding and utilization of the system's functionalities, as well as prompt support in case of issues or inquiries.

Audit and Reporting: The system should have a robust audit and reporting capabilities to track and document all activities and transactions processed by the system, including suspicious activity reports (SARs), to meet regulatory requirements and facilitate auditing and reporting to relevant stakeholders.

2.6. General Technical Requirements

2.6.1. Language Support: All information technologies must provide support for the ***either national or business language(s) of the end-user(s)***.

2.6.2. Electrical Power: All active (powered) equipment must operate on ***Not applicable.***

2.6.3. Environmental: Not applicable

2.6.4. Safety: Not applicable

3. SERVICE SPECIFICATIONS – SUPPLY & INSTALL ITEMS

3.1. System Analysis, Design and Customization/Development

3.1.1. The Supplier MUST perform the following Analysis and Design activities using a formal system analysis/development methodology with the following key activities and design deliverables.

3.1.1.1. Detailed Analysis: ***Process Design Document; Software/System Test Descriptions; Software/System Test Plan***

3.1.1.2. Physical Design: ***Interface Design Document***

3.1.1.3. Integrated System: ***User's Manual; Operations Manual***

3.2. Software Customization / Development

3.2.1. The Supplier MUST perform Software Customization / Development using a formal software development methodology with the following characteristics and/or with the following technologies and/or tools.

3.2.1.1. The supplier is free to choose any methodology that supports agile delivery.

3.3. System Integration (to other existing systems)

3.3.1. The Supplier MUST perform the following Integration Services:

- Configurable integrations to project systems

3.4. Training and Training Materials

3.4.1. The Supplier MUST provide the following Training Services and Materials.

3.4.1.1. User: ***minimum curricula, modes of training, modes of testing, and training materials for: the introduction to computers, the operation of the relevant equipment incorporated in the System, as well as the operation of the Software applications incorporated in the System.***

3.4.1.2. Technical: ***minimum curricula, modes of training, modes of testing (e.g., certification levels), training materials and training locations for: the key technology and methodology components of the Information System***.

3.4.1.3. Management: ***minimum curricula, modes of training, modes of testing, training materials, and training locations for the familiarization with the functionality, technology, and methodology components of the Information System, corporate management of information systems***.

3.5. Data Conversion and Migration

3.5.1. The Supplier MUST provide services and tools to perform the following Data Conversion and Migration Services:

- Bulk upload of data, to enable import from historical system and aggregator databases.

3.6. Documentation Requirements

3.6.1. The Supplier MUST prepare and provide the following documentation.

3.6.1.1. End-User documents:

- The supplier should provide handbooks, administration guides, user operation schedules, video demos.

3.6.1.2. Technical documents:

- The supplier should provide system custodian operation schedules.

3.6.2. The document format should include:

- Detailed documentation of the modules.
- Graphical representation or screen capture of input forms, messages and reports
- Online help documentation accessible from the system through a clickable menu item or icon

3.7. Requirements of the Supplier's Technical Team

3.7.1. The Supplier MUST maintain a technical team of the following roles and skill levels during the Supply and Installation Activities under the Contract:

3.7.1.1. Project Team Leader: *supplier to determine*

3.7.1.2. Business Analyst: *supplier to determine*

3.7.1.3. System Analyst: *supplier to determine*

3.7.1.4. Database Expert: *supplier to determine*

3.7.1.5. Programming Expert: *supplier to determine*

3.7.1.6. System Administration / Security Expert: *supplier to determine*

3.7.1.7. Computer Hardware Expert: *supplier to determine*

3.7.1.8. Network and Communications Expert: *supplier to determine*

3.7.1.9. Training Expert: *supplier to determine*

3.7.1.10. Documentation Specialist: *supplier to determine*

3.8. Telecommunications Services (Supplier-provided)

3.8.1. The Supplier MUST provide the following Telecommunications Services: Not applicable.

4. TESTING AND QUALITY ASSURANCE REQUIREMENTS

4.1. Inspections

4.1.1. Factory Inspections: *Not applicable*

4.1.2. Inspections following delivery: *Not applicable*

4.2. Pre-commissioning Tests

In addition to the Supplier's standard check-out and set-up tests, the Supplier (with the assistance of the Purchaser) must perform the following tests on the System and its Subsystems before Installation will be deemed to have occurred and the Purchaser will issue the Installation Certificate(s)

- The system should undergo comprehensive testing to ensure compliance with functional and non-functional requirements.
- Test cases should be developed and executed to verify the accuracy, reliability, and performance of the system.
- The system should undergo penetration testing to identify and address potential security vulnerabilities.
- Regression testing should be performed after system updates or changes to ensure the stability and functionality of the system.
- Documentation of test results, including issues identified and their resolutions, should be maintained for reference and auditing purposes.

4.2.1. System Setup

Tests	**Test summary**
Super admin access	A super admin with credentials can access the web portal admin page
User group creation	Create Group that accepts permissions. Available permissions based on all functions
User creation	Create the user Add the user to a group User logs in the system Positive and negative permission test
Organization creation	Create a new Entity

	Configure entity permissions
Web access	Users Can access via web browser
Process approvals	Test maker checker functionality
Data imports	Upload data in bulk
Data exports	Export data in bulk
Multi tenancy	The system instruction language can change based on configuration The system transactional currency can change based on configuration The system locations can change based on configuration

4.2.2.

Test	**Test Summary**
Functional Testing	All features and functions of AML tested
Usability Testing	Ease of use and friendliness
Security testing	Protection against unauthorized access

4.2.3. Reports

Test	**Test Summary**
Data analytics reports	Dashboard Metric monitoring reports

4.3. Operational Acceptance Tests

The Purchaser (with the assistance of the Supplier) will perform the following tests on the System and its Subsystems following Installation to determine whether the System and the Subsystems meet all the requirements mandated for Operational Acceptance.

Test	**Test Summary**
Create	Adding required data for all the functional modules
View	All relevant fields are viewable based on function
Edit	All relevant fields are editable based on function
Delete/Archive	All relevant fields can be archived based on function
Database response time	Quick pull and push requests
Integration	Test integration with PowerBi

5. SERVICE SPECIFICATIONS – RECURRENT COST ITEMS

5.1. Warranty Defect Repair

5.1.1. The Supplier MUST provide the following services under the Contract or, as appropriate, under separate contracts (as specified in the RFP documents).

- An administrative task for periodic update shall be provided to allow for fixing patches and upgrades of the software.

5.1.1.1. Warranty Defect Repair Service:

- ***coverage period – 6 months***
- ***response time – 4 hours***
- ***problem-resolution performance standards – 2 business days***
- ***modes of service – Online support and telephone***

5.2. Technical Support

5.2.1. The Supplier MUST provide the following services under the Contract or, as appropriate, under separate contracts (as specified in the RFP documents).

5.2.1.1. User support / hotline: *purchaser provided.*

5.2.1.2. Technical Assistance: *Supplier to provide in line with SLA below.*

5.2.1.3. Post-Warranty Maintenance Services: *This will be subject to a separate contract.*

5.2.1.4. Service Level Agreement: A detailed service level agreement shall specify the priority levels (low, medium and high), response time based on priorities and order of support escalation.

Priority	Description	Response Time	Resolution Time
High	Critical system is down. Functions not usable. No workaround or alternative is available. Data is corrupted. Many end users are affected. Regulatory/legal deadlines will be missed.	15 Minutes	4 Hours
Medium	Some functions are usable with severe restrictions. No workaround or alternative is available. Several end users affected.	1 Hour	8 Hours
Normal	Basic functions are usable with minor restrictions. Workaround or alternative is available. One or more users affected.	1 Hour	3 Days
Low	Minor problem. Functions are usable. Defect is cosmetic or simply a nuisance.	Next Business Day	5 Days

5.3. Requirements of the Supplier's Technical Team

5.3.1. The Supplier MUST provide a technical team to cover the Purchaser's anticipated Post-Operational Acceptance Technical Assistance Activities Requirements (e.g., modification of the Information System to comply with changing legislation and regulations) with the roles and skill levels that are specified below. The minimum expected quantities of inputs by the Supplier's technical support team are specified in the relevant System Inventory Tables for Recurrent Cost Items.

5.3.1.1. System Analyst: *Supplier to determine*

5.3.1.2. Database Expert: *Supplier to determine*

5.3.1.3. Programming Expert: *Supplier to determine*