



REQUEST FOR EXPRESSION OF INTEREST (REOI)

for the Procurement of a System for Automating ML/FT and Sanctions Compliance Risk Assessment and Monitoring

1. Purpose of the Request

The Central Bank of Armenia (CBA) is seeking expressions of interest and constructive feedback from experienced vendors regarding the upcoming procurement of a system aimed at automating the processes of ML/FT and sanctions compliance risk assessment and monitoring.

A draft Terms of Reference (ToR) has been developed to outline the anticipated technical, functional and implementation requirements. Before initiating a formal tender process, we are conducting this REOI to:

- Identify parties potentially interested in participating in the forthcoming tender and
- Collect feedback on the draft ToR, including its feasibility, clarity, realism, completeness and potential implementation limitations.

This consultation will allow CBA to fine-tune the ToR and procurement structure to ensure a competitive, practical and efficient tendering process.

****This REOI is not a solicitation for bids, but rather a preliminary step to assess the interest of vendors to deliver such a system. Vendors expressing interest may be invited to submit proposals in a forthcoming formal tender.***

2. Overview of the Draft Project Scope

The attached draft ToR outlines the following major features:

- Automation of data collection from financial institutions via surveys or system integrations;
- Customizable risk models (inherent, control/management quality, residual risk);
- Integration with external systems/databases (ETL, APIs);



- Dashboarding, anomaly detection, trend analysis, machine learning capabilities;
 - Strong role-based access control, audit logging and multi-factor authentication;
 - Full on-premise deployment (no cloud);
 - Compliance with international standards (e.g. ISO 27001, FATF guidelines);
 - Support for multi-phase data collection across multiple supervised sectors.
-

3. Request to Respondents

CBA kindly invites all interested organizations to:

- Express interest in the upcoming procurement,
- Review the draft ToR, and
- Submit any comments, suggestions or concerns regarding:
 - Technical feasibility or practicality of the requirements;
 - Any implementation or deployment risks foreseen;
 - Missing elements or over-specifications;
 - Potential licensing, localization or integration challenges;
 - Proposed evaluation criteria (if deemed restrictive or too vague).

Your insights will be highly valuable in helping us finalize a fair, inclusive and implementable tender.

4. Tender Participation Requirements & Eligibility

The following eligibility conditions may apply to participants in the forthcoming tender, in accordance with the Law on Procurement of the Republic of Armenia:

Ineligible Participants

- Have been declared bankrupt by a court;
- Have been convicted (within the last 5 years) of terrorism financing, child exploitation, human trafficking, bribery, or other crimes related to economic activity (unless expunged);
- Have a final administrative ruling against them for anti-competitive behavior, abuse of dominant position, or unfair procurement practices within the last 3 years;



- Are on the Eurasian Economic Union (EEU) black list (unless this procurement is funded under an international agreement);
- Are on Armenian procurement black lists.
Affiliated persons or entities, including those founded by the same individuals or having more than 50% joint ownership, may not participate simultaneously, unless through a formal joint venture (JV).

The subsequent tender will include:

- Bid Security: Expected to be ~5% of financial proposal in the form of cash or banking guarantee,
 - Contract Execution Security: Typically, 10% of contract value in the form of cash or banking guarantee.
-

5. Submission Requirements

Please provide:

- A short expression of interest confirming your willingness to participate in the future tender;
- Any feedback, observations, or suggestions on the draft ToR;
- The anticipated timeframes required for completion of the works.
- Contact details (organization name, contact person, email, phone) responsible for REoI Q&A session, as well as for receiving the formal tender invitation when launched.

****There is no need to submit supporting documents, financial quotes, or company credentials at this stage.***

6. Submission Instructions

-  Please send your feedback by 05th of September, 2025.
 -  Submit via email to: procurement@cba.am, with CC to edgar.begrakyan@cba.am
Subject: Expression of Interest – AML/CFT System
-

7. Confidentiality and Non-binding Nature



Participation in this REol is non-binding and does not represent a commitment to submit a proposal in the future tender. All responses will be treated confidentially and used solely for internal planning and refinement of tender documentation.

8. Contact for Clarifications

For any questions or to request the draft ToR:

Mr. Edgar Begrakyán

Coordinator, Financial Supervision and Licensing Department

Central Bank of the Republic of Armenia

✉ edgar.begrakyan@cba.am

☎ +374 10 592 592

***Published on
August 20th, 2025***

Ms. Siran Yeganyan

Head of Procurement Coordination Service

Central Bank of the Republic of Armenia

✉ siran.yeganyan@cba.am

☎ +374 10 592 592



Appendix

TECHNICAL PROPOSAL FOR SYSTEM PROCUREMENT WITHIN THE FRAMEWORK OF THE ML/FT AND SANCTIONS COMPLIANCE RISK ASSESSMENT AND MONITORING AUTOMATION PROJECT

TECHNICAL AND FUNCTIONAL SPECIFICATIONS

INTRODUCTION

The Central Bank of the Republic of Armenia (hereinafter also referred to as the Bank or the CBA) is a legal entity authorized to carry out public functions. The Bank's primary objectives are to ensure price stability and financial stability in accordance with the Constitution of the Republic of Armenia and the RA Law on the Central Bank of Armenia. The CBA develops and implements monetary policy programs, regulates and supervises the financial system, oversees the payment system, ensures the issuance and circulation of the national currency, combats money laundering and terrorism financing, manages Armenia's international reserves, and performs other related functions.

This project aims to significantly enhance the Bank's capabilities in combating money laundering (ML) and the financing of terrorism (FT), as well as in ensuring compliance with international sanctions, by employing supervisory technologies (hereinafter also referred to as SupTech).

OBJECTIVE

The purpose of this request for proposals is to identify a vendor capable of providing a comprehensive software solution (hereinafter referred to as the "System"), including its deployment, configuration, training, and ongoing support and maintenance following implementation.

The System should enable the effective identification, assessment, and management of ML/FT and international sanctions compliance risks through the use of advanced technological tools.



Upon implementation of the project, the following requirements in the processes of ML/FT and sanctions compliance risk assessment and monitoring are expected to be fulfilled:

- Automation of data collection (including via surveys), export, and quality checks;
- Capability for integration with other systems and databases;
- Automation of risk assessment for inherent and residual ML/FT and sanctions compliance risks based on data, categorized by financial institutions (FIs), sectors, and the financial system as a whole;
- Automation of early warning or red flag mechanisms;
- Implementation of continuous monitoring capabilities for FI and sector-specific trends (preferably including the ability to detect anomalies and predict future risks at the FI, sector, and/or system level);
- Capability for comparative analysis between FIs and across sectors;
- Support for national-level ML/FT and sanctions compliance risks assessment;
- Introduction of various reports, dynamic dashboards, and a user-friendly UI/UX platform to significantly enhance supervisory insight.

PLACE OF IMPLEMENTATION

The implementation site for the project is the Central Bank of the Republic of Armenia, located at 6 Vazgen Sargsyan Street, Yerevan, 0010, Republic of Armenia.

IMPLEMENTATION LOCATION

The System must be deployed within the internal infrastructure (on-premises) of the Central Bank. Cloud-based solutions are not acceptable.

SCOPE OF WORK/REQUIREMENTS

This section presents the minimum requirements for the System. The scope of work can be divided into the following sections.

5.1. General Requirements

The System must be a pre-developed (standardized) solution, available in the form of off-the-shelf software on the market, without the need for significant customization. The System must be



designed for rapid deployment, include all necessary files and instructions for installation in the target environment, and be customizable.

5.2.Data Management

Data Entry: The System must allow the entry of information necessary for the assessment of AML/CFT and sanctions compliance risks through an automated survey generation platform, by receiving MS Excel and other standardized file types, and through permissible databases and external systems.

Survey Management: The System must provide a secure and user-friendly platform for the use of questionnaires intended for collecting information from reporting financial institutions (FIs). Upon receiving an invitation link, FIs must be able to access the platform to input the required information, save it, and submit their responses. The platform must offer multilingual support, real-time data validation, and automated email notifications, including invitations, deadline reminders, and confirmations of successful questionnaire completion. Additionally, it must provide daily statistical data on questionnaire activity. The platform should be able to manage multiple supervised sectors and various questionnaires from different reporting FIs. For security purposes, the software solution must be deployed within the user's own infrastructure, supporting two-factor authentication, without reliance on cloud services. It must include login monitoring, lockout controls, and notifications to both FIs and supervisors in the event of account lockouts. It should also be capable of encrypting sensitive data and must undergo security testing by third-party security specialists. The platform must minimize the reporting FIs' workload through features such as mass copy-paste from Excel and conditional questioning, where only relevant questions are shown, reducing the total number of questions FIs must answer. Data must be validated in real-time, with alerts displayed directly within the questionnaire. The requirements for data validation and form completeness must minimize one of the major issues related to AML/CFT reporting: data quality. The platform must reduce or even eliminate quality issues such as incomplete reports, erroneous data, human errors, missing data validations, data usability transformation problems, and the resulting wasted resources—factors that are among the largest resource drains in the risk assessment process. The platform must streamline the survey data



collection process. Data collected from surveys must be imported into risk models without requiring additional manual manipulation, aggregation, or transformation by supervisors. In other words, survey data must be automatically imported into the risk model, with risk scores calculated within seconds at the push of a button, saving significant time and resources.

Support for MS Excel and Other Standardized Files: The System must accept information from MS Excel and other standardized files for the comprehensive assessment of AML/CFT risks and the quality of their management. These files must follow a pre-defined template to ensure the standardization of all submissions. The System must support automatic data importation from Excel and other standardized file formats, eliminating the need for manual data entry. After uploading a file, the System must automatically map and validate the data according to pre-established rules. It must also support integration with data analysis tools, enabling supervisors to analyze the submitted data for risk assessment and compliance purposes.

Integration with Various Databases and Systems: The System must support integration with external systems through APIs and implement secure authentication mechanisms for API connections. It must also be capable of automatically surveying different databases, downloading, transforming, and loading (ETL) data, thereby eliminating the need for manual data entry or transformation, reducing the likelihood of errors, and improving efficiency. The results of these surveys must be directly linked to risk models, enabling rapid updates to risks assessments.

5.3.Roles and Permissions

The System shall implement multi-factor authentication (MFA), requiring two or more authentication methods for access (e.g., a password plus a one-time code sent via SMS or email). All sensitive data must be encrypted using strong algorithms during both transmission and storage, preventing unauthorized access even in case of data interception. Role-based access control (RBAC) must be applied, ensuring that users can only access the data and functions appropriate to their roles, thereby reducing the risk of misuse. Additionally, the System must maintain logging and monitoring of user activities, tracking login attempts, data modifications, and other critical actions to detect suspicious behavior.

5.4.Risk Modeling and Analysis



In the System, users must be able to create customized models for inherent risk and control/management quality based on sector-specific AML/CFT risk factors. They should also be able to manage questionnaires and data input through the System's data management functionality. The solution must provide configurability for inherent risk and control/management quality models, allowing users to edit models and view the current status of calculations. Supervisors must be able to calculate inherent risk, control/management quality, and residual risk at both the individual financial institution (FI) and sector levels. The final output is a residual risk heatmap, providing supervisors with a comparative sectoral overview, enabling risk-based prioritization of supervisory actions—specifically targeting high-risk institutions and high-risk sectors/factors. Supervisors must also be able to conduct qualitative assessments by inputting new information obtained during off-site or on-site supervision. This new information may relate to adjustments in the automatically calculated inherent risk or updates to the control/management quality assessments. The System must support the preservation of model versions over time, meaning previous versions of models must be stored to allow supervisors to compare new model evaluations with past ones at any time. The comprehensive dataset collected through questionnaires will aid supervisory activities even after the reporting cycle ends, enabling the execution of analyses and generation of statistical data at various levels, including:

- Risk factor level,
- Individual FI level (with comparative analysis to similarly sized FIs or the entire sector),
- Jurisdiction level,
- Country group level (e.g., FATF lists), and
- Sectoral levels.

The System must also offer threshold selection assistance, which plays a critical role in the risk assessment functionality.

When multiple reporting cycles are available, the System must provide trend analysis capabilities for individual FIs and for the overall financial system/sector. The System should be capable of integrating machine learning and artificial intelligence (AI) technologies to learn from historical data and improve the accuracy of risk predictions. As a result, the System can offer predictive analytics to not only understand current risks but also anticipate future risks based on past data



and trends. Furthermore, the System must incorporate dynamic dashboards that provide a comprehensive view of sector-wide risk factors and trends. Summary dashboards must allow users to compare risks across different FIs or sectors, identifying patterns or anomalies. Users should often have the ability to customize dashboards to focus on specific criteria, time periods, or areas of interest.

5.5. Reporting

The System must support the creation of customized reports, allowing supervisors to generate reports for analysis and management across various risk factors, institutions, and sectors, and at different frequencies (e.g., daily, monthly, quarterly). Users must be able to select parameters and apply filters (e.g., based on time periods, sectors, or jurisdictions) to tailor the reports to their needs. The System must generate both visual reports (e.g., charts) and tabular reports that show data values over time. It must support both scheduled and on-demand report generation and offer pre-designed templates, allowing users to create and save custom templates for regular use. Reports must be exportable in user-preferred formats, including MS Excel, PDF, CSV, or MS Word. The System must validate the data to ensure consistency and must update reports as new data is imported. Role-based access control must restrict who can create, edit, or view reports, maintaining security and compliance. All of this will provide supervisors with the tools to efficiently generate accurate and targeted reports for data-driven decision-making.

5.6. Workspace

The System must feature a user-centered design that ensures an intuitive and seamless experience for employees. The interface must be visually simple, easy to navigate, and customizable, allowing users to tailor dashboards, alerts, and reports according to their preferences. The design must ensure that all key functions are accessible within the same window, minimizing disruptions and cognitive load. To maximize efficiency, the System must also provide smooth integration with external platforms and databases. The System must include a robust change management process overseen by supervisors, ensuring approval workflows are in place for any changes. This requirement guarantees that all critical changes—whether related to risk thresholds, alerts, reports, or user roles—are controlled, approved, and logged.



DESCRIPTION OF FUNCTIONAL REQUIREMENTS

No.	Requirement	Description	Examples
1	<u>Surveys and Data Management</u>		
1.1	Ability to Easily Create and Customize Specialized Surveys	• The System should allow users to create new surveys for the assessment of AML/CFT and sanctions compliance risks, customizing the questions, answer formats, and structure based on specific objectives or data needs. • The System should provide a clear and simple interface that enables even non-technical users to design, customize, and deploy surveys without requiring extensive technical knowledge. • Surveys should include conditional logic, branching options, and multilingual support, making them flexible for different situations. • <i>Add, edit, or remove questions:</i> Users should be able to quickly add new questions, modify existing ones, or remove questions that are no longer needed. This allows for dynamic updating of surveys without the need to start from scratch. • <i>Enable or disable questions:</i> Users should be able to enable or disable individual questions without deleting them, providing flexibility to adapt surveys for different scenarios. For example, it should be possible to disable certain questions for specific	



		FIs while maintaining flexibility in data collection. • <i>Change the hierarchy of questions:</i> The System should allow users to modify the hierarchy of questions, enabling better organization of the surveys. For example, it should be possible to group questions by topic or complexity to ensure logical sequencing. • <i>Reorder the sequence of questions:</i> Users should be able to rearrange the order of questions within a survey, facilitating easier adjustment of the survey flow based on feedback or shifting priorities.	
1.2	Ability to Easily Distribute and Collect Surveys, and Automatically Aggregate the Results	• The System should allow users to easily distribute surveys through various channels (e.g., email, web portals, etc.), ensuring efficient delivery to the target financial institutions. • After distribution, the System should automatically collect responses without requiring manual intervention. It should be able to track who has completed the survey and send reminders to those who have not. • The System should automatically aggregate the results in real time, enabling users to view and analyze data as soon as responses are submitted. This helps save time and provides instant insights. • It should be possible to use aggregated data to generate custom	



		reports and dashboards, offering a clear visual representation of survey outcomes. • The System should ensure secure storage of collected data by enforcing access controls to protect the integrity and confidentiality of survey responses.	
1.3	Survey Field Properties	• <i>Question Text:</i> This should be the primary text displayed to the respondent. • <i>Additional Description or Help Text:</i> This field should provide supplementary information or instructions to guide the respondent. It may clarify the context of the question or include specific instructions, such as “Select all that apply” or “Provide a numeric response.” • <i>Rich Text Editor:</i> The System should provide formatting options for question text and instructions—such as bold, italic, underlining, lists, etc. This helps emphasize key parts of the question or guidance for better comprehension. • <i>Links to Resources:</i> The question field may include hyperlinks to external resources or documents, giving the respondent access to additional materials or contextual information relevant to the question.	
1.4	Types of Data Collected from Responses	• <i>Number:</i> Allows the collection of simple numeric values (e.g., quantities, scores).	



		• <i>Currency</i>: Supports the entry of monetary values, formatted as currency. • <i>Percentage</i>: Used to collect percentage values. • <i>Segmented Numeric Data</i>: Numeric entries categorized by jurisdiction, region, or any custom segmentation (e.g., sales by country, income by department). • <i>Calculated Field</i>: Represents a relationship between two numeric values. Automatically computes and displays the ratio or result between them. • <i>Sum of Other Fields</i>: Automatically calculates the total of selected numeric fields. • <i>Binary</i>: Captures yes/no or true/false type responses. • <i>Multiple Choice</i>: Allows respondents to select one or more options from a list (e.g., radio buttons for single selection or checkboxes for multiple selections). • <i>Date</i>: Collects specific dates in a standard format (e.g., DD/MM/YYYY). • <i>Free Text</i>: An open text field that allows respondents to enter unstructured textual responses. • <i>Country Selector</i>: A dropdown menu that allows respondents to select a country from a predefined list. • <i>Custom Dropdown</i>: A configurable dropdown list for selecting from predefined options, such as industry	
--	--	---	--



		sectors, product types, or custom categories. • <i>File Upload</i>: Allows respondents to upload files or documents as part of their response (e.g., PDFs, Word documents).	
1.5	Survey Completion Features Based on Conditional Question Logic	• The System should show or hide questions during the survey based on previous responses. This improves the user experience by displaying only relevant questions tailored to the respondent's situation, simplifying the completion process. • A given question should be able to depend on a "Yes" answer to another question, such that if the respondent selects "Yes," the dependent question is displayed. • Similarly, the System should permit certain questions to appear only if the response to another question is "No." This allows follow-up logic based on negative responses. • A given question should be able to depend on multiple prior answers, appearing only when certain combinations of "Yes" and/or "No" responses are given. This enables complex logic and personalized flows based on multiple conditions. • A question should be able to depend on another question, which in turn depends on another, and so on. This allows for deeply personalized multi-layered survey paths driven by sequences of answers.	



		• Jumping to the next/previous unanswered question: The questionnaire should allow users to quickly navigate to the next or previous unanswered question, ensuring that mandatory questions are not skipped and improving the experience—especially in longer surveys. • Bulk data entry: Users should be able to enter large sets of data in one go, which is especially useful when recording multiple or repetitive entries. • Export of survey to .xlsx or .pdf formats: After completing the survey, users should be able to download their responses in Excel (.xlsx) or PDF format. This allows them to save a formatted copy, share their answers, or use the data for further analysis.	
1.6	Validation of Survey Data Quality and Completeness	• The System should be able to perform automatic checks to ensure that all required fields are filled out. This ensures data completeness by verifying that the respondent has provided input for all mandatory questions or sections before the survey is submitted. • The platform should allow validation rules to be defined for individual data points. For example, it should be possible to set acceptable ranges for numeric fields, define formats for date fields, or restrict certain inputs to predefined values (e.g., percentages	For example, if one field indicates a start date and another an end date, the System should be able to validate that the end date is later than the start date.



		within the 0–100 range). This ensures that each data point meets specific quality standards. • The System should also support customizable data validation rules that involve relationships between two or more data fields.	
1.7	Antivirus Scanning	• Automatic Scanning on File Upload: When a file is uploaded, the System should automatically scan it for known viruses, malware, and other security threats using integrated antivirus software. • Execution-Based Scanning: The antivirus scan should be triggered upon execution of the file upload process. • Real-Time Alerts on Detection: If a malicious file is detected, the System should notify administrators or users in real time, enabling immediate action—such as rejecting the file or issuing a warning to the user. • Supported File Types: The antivirus scanning capability should cover a variety of file types (e.g., PDF, images, Word documents, spreadsheets) to ensure comprehensive protection. • Regular Updates: The antivirus engine should be updated regularly with the latest virus definitions to detect emerging threats effectively.	
1.8	Survey Rejection and Feedback	• Rejection of Invalid Submissions: The System should allow supervisors to	



		reject submitted surveys that do not meet predefined requirements or contain errors. This ensures that only accurate, valid, and complete data is processed. Automated Feedback with Rejection Reason: Upon rejecting a survey, the System should enable the supervisor to communicate the specific reason for rejection to the respondent. This may be done through automated notifications or messages indicating which part of the survey must be corrected (e.g., missing data, invalid entries, or inconsistent responses).	
1.9	Survey Resubmission and Correction Workflow	- Access to Rejected Surveys for Resubmission: The System should allow users to re-access and edit rejected surveys at any time after they are returned for correction. Users should be able to resume the survey from the point of rejection and make necessary updates. - Preservation of Previously Entered Data: All previously entered data should remain saved. Users should not be required to re-enter the entire form but may correct only the fields or sections flagged during the rejection process, streamlining the correction workflow. - Highlighted Fields Requiring Correction: The System should highlight or clearly mark the specific fields or sections that require	



		correction, based on the rejection reason provided. This guides the respondent directly to the problematic inputs, reducing confusion. • Resubmission Without Restarting: After making the necessary corrections, users should be able to resubmit the survey without having to restart from scratch. This ensures a smooth and user-friendly correction and resubmission process for both respondents and reviewers.	
1.10	Multi-Phase Survey Functionality	• Support for Multi-Phase Data Collection: The System should allow surveys to be conducted across multiple phases or time periods. This enables data collection at different stages of a program or project, supporting iterative or longitudinal analysis. • Carry-Forward of Previous Responses: The System should allow responses from earlier phases to be carried over into subsequent survey phases. This reduces respondent burden by eliminating the need to re-enter unchanged data. • Change Tracking Across Phases: The System should track changes made to responses between phases. This allows supervisors or analysts to monitor how responses evolve over time, which is especially useful for long-term studies or monitoring cycles. • Adaptive Questionnaire Configuration:	



		Each phase of the survey should be configurable independently. The System should support adding new questions, modifying existing ones, or updating formats based on insights gained from previous phases. This iterative approach improves data relevance and quality. • Cross-Phase Analytical Capabilities: The System should support comprehensive analysis across multiple phases, enabling insights into trends, patterns, and changes over time. Visualization and comparison tools should help identify shifts in responses and emerging risks.	
1.11	Organizational List Management and Synchronization	• Editable Organization Records: The System should allow supervisors to easily update the list of organizations when changes occur in organizational data (e.g., name, contact information, or status). This ensures that all organizations included in the survey distribution list remain current and relevant. • Add, Update, or Remove Organizations: Users should be able to add new organizations, update the information of existing ones, or remove outdated entities. This guarantees the accuracy of the organization list used for distributing surveys. • Resend Surveys After Organization Updates: After the organizational list is	



		updated, the System should allow the resending of surveys to the affected organizations. This ensures that newly added or updated entities receive the latest surveys or follow-up communications. The System may also trigger automatic reminders or notifications to these updated organizations to ensure timely completion. • Synchronization with Distributed Surveys: All changes made to an organization's data should be automatically synchronized with previously distributed surveys. This ensures that collected data remains linked to the most up-to-date organizational records, preserving data integrity.	
1.12	Notification and Messaging Features	• <i>Invitations:</i> Automated emails or alerts that invite participants to take part in a survey, task, or process. These messages should include a personalized note and a link to the relevant form or System. • <i>Reminders:</i> Automated reminders should be sent if the user has not completed the required action (e.g., submitting a survey). The System may send multiple reminders over a defined period to prompt timely completion. • <i>Deadline Extensions:</i> Notifications that inform participants about an extension of the deadline for completing or	



		submitting a form. This ensures all parties are aware of schedule changes. • <i>Password Reset</i>: Automated messages sent when a user requests a password change. These messages should include secure instructions and a link to reset the password. • <i>Submission Confirmation</i>: Users should receive confirmation notifications once a task, survey, or form is successfully submitted. This assures them that their input was received successfully. • <i>Account Lockout</i>: Notifications should be sent when a user is locked out of the System due to repeated failed login attempts or security violations. The message should provide instructions on how to restore access.	
1.13	Email Branding and Customization	• <i>Logos and Colors</i>: Emails should be customizable with the organization's logo, brand colors, and visual identity. This ensures that all communications are immediately recognizable and reinforces the Central Bank's brand presence. • <i>Email Header/Footer</i>: Each email should support a customizable header and footer that includes the Central Bank's name, contact information, and links to relevant pages such as the website or privacy policy. • <i>Fonts and Styles</i>: The System should allow the use of specific fonts and text	



		styles to ensure consistency with the Central Bank’s visual identity across all communications.	
1.14	Survey Engagement Status Notifications by Institution	• <i>Inactive Financial Institutions (FIs):</i> The email should indicate which financial institutions have not yet started the survey or have remained inactive since receiving the invitation. This helps administrators monitor non-responding FIs and take appropriate actions, such as sending reminders or initiating further communication. • <i>Active (In-Progress) Financial Institutions:</i> The System should distinguish those FIs currently working on the survey but who have not yet submitted their responses. This insight is critical for tracking progress and ensuring that institutions remain engaged in the process. • <i>Submitted Financial Institutions:</i> The email should include a list of FIs that have successfully completed and submitted their surveys. This helps administrators and supervisors keep track of which institutions have fulfilled their obligations.	
1.15	Supervisor Access to In-Progress Surveys	• <i>Progress Monitoring of Partially Completed Surveys:</i> Supervisors should be able to monitor the progress of surveys that have been partially completed. The System should display which sections are	



		filled and which remain incomplete. This visibility allows supervisors to assess ongoing work and intervene when necessary. • <i>Real-Time Guidance and Feedback:</i> Supervisors should have access to view in-progress responses and provide respondents with real-time feedback or guidance. This feature ensures that responses meet quality and completeness standards before final submission. • <i>Deadline Tracking and Reminders:</i> Supervisors should be able to monitor approaching deadlines and the overall completion status of each respondent. The System should allow for sending reminders to users whose survey submissions are pending as the deadline approaches.	
1.16	Use of MS Excel and Other Standard Files for ML/FT Inquiries	• <i>File Acceptance:</i> The System should be able to accept MS Excel and other standardized file types for the purpose of assessing ML/FT risks and the quality of their management. These files must follow pre-defined templates to ensure consistency across all submissions. • <i>Data Validation:</i> Upon upload, the System should validate the data to ensure all required fields are completed and the content conforms to the expected structure (e.g., correct currency formatting, valid date formats).	• The template should include the required fields, such as the volume of cash transactions, the number of suspicious transactions,



		• <i>Validation Rules:</i> Validation rules should include checks for missing data, duplicate entries, and incorrect formats. The System must enforce data integrity before further processing. • <i>Data Mapping and Processing:</i> Once validated, each data element (e.g., amounts, entity names, risk levels) should be accurately mapped to the System's internal fields for storage and analysis. • <i>Automation and Integration:</i> The System should support automated import of data from Excel and other standard file formats, eliminating the need for manual entry. Upon upload, the System should automatically map and validate the data using pre-configured rules. • <i>Integration with Analytical Tools:</i> The System should support integration with analytical tools, enabling supervisors to analyze submitted data for risk assessment and compliance evaluation. • <i>Error Handling and Messaging:</i> If errors are detected in the submitted Excel or standard file (e.g., missing fields, formatting issues), the System should notify the user with clear error messages indicating what needs correction. • <i>File Resubmission Workflow:</i> The System should provide a resubmission process that allows users to upload	the number of resident and non-resident clients, and other relevant data.
--	--	--	---



		corrected files after validation failures. • <i>Template Version Control and Data Update Support:</i> The System should implement version control to manage updates to Excel and other standardized file templates. When configurations change, updated templates must reflect the latest format and data requirements.	
1.17	API Integration	• <i>API Connectivity Support:</i> The System should support integration with external systems via API for both data ingestion and data sharing. • <i>Secure Authentication for API Connections:</i> The System should implement secure authentication mechanisms for establishing API connections. It must also support secure file transfer, particularly using SFTP (Secure File Transfer Protocol). • <i>Error Handling and Retry Mechanisms:</i> The System should include error handling capabilities and automated retry mechanisms for failed API requests to ensure data consistency and reliability. • <i>Data Mapping from API Inputs:</i> Upon receiving data via API, the System should map external data structures to its internal data model to ensure proper storage and use. • <i>Automated and Scheduled API Queries:</i> The System should support automated execution of API requests based on a configurable schedule, enabling timely and efficient data	



		exchange. • API Request Logging and Traceability: The System should maintain a complete log of all API interactions, including request details, response status, and any associated errors for audit and troubleshooting purposes.	
1.18	Automatic ETL Performance from Various Databases and Import of Query Results into Risk Models	• <i>Extract (Data Download):</i> The System should automatically extract collected survey data according to a user-defined schedule (e.g., daily, weekly). This extraction may include responses, metadata, and other relevant details from various formats or platforms. • <i>Transform (Data Preparation):</i> After extraction, the System should transform the data to make it suitable for analysis and integration with risk models. This process may involve data cleaning, normalization, and restructuring to ensure consistency and accuracy. • <i>Load (Integration with Risk Models):</i> The transformed data should be loaded into the System's risk models, where it will be used for updating risk scores, profiles, or monitoring thresholds. • <i>Real-Time Updates:</i> The System should update risk models immediately upon completion of the ETL process, ensuring that risk assessments reflect the most current data from survey results.	



2. <i>Risk Modeling</i>			
2.1	Risk Assessment (Inherent Risk, Controls, and Residual Risk)	• Inherent Risk Data Collection and Assessment: The System should provide functionality for inherent risk assessment using predefined indicators (such as customer risk, geographic risk, and product/service risk) or customizable models. These models should support automated risk scoring based on risk factor inputs. The overall inherent risk assessment of the institution is a combination of the institution-specific inherent risk and the sector-level inherent risk evaluations. • Collection and Evaluation of Control Measures / Quality of Risk Management: The System should support the collection and evaluation of data on risk mitigation measures and control effectiveness, such as internal audit practices, transaction monitoring systems, and customer due diligence (KYC) processes. The System shall generate a control quality score indicating the effectiveness of these controls in reducing inherent risk. • Residual Risk Calculation: The System should be capable of automatically calculating residual risk by factoring in the assessed inherent risk and the effectiveness of applied control measures. Formula: Residual Risk = Inherent	For example, in the ML/FT context, inherent risk data may include the customers' jurisdiction, as well as transaction type and volume. The System should assess inherent risk based on these indicators. For example, if a financial institution has an effective transaction monitoring System and strong KYC procedures, the System should assign a high control quality score—indicating that risks are being well-managed. For example, if a high inherent risk is identified—due to large transaction volumes in a high-risk jurisdiction—but effective controls are in



		Risk – Control/Management Quality Score	place, the residual risk may be significantly reduced.
2.2	Risk Weighting and Aggregation	• Different risk factors—such as customer type, legal framework, nature of transactions, and product/service risk—should be assigned different weights to reflect their relative importance. • Weighted averages shall be used to calculate the overall risk score, based on ML/FT risk indicators. This ensures a balanced and quantitative approach to risk assessment.	For example, 50% weight could be assigned to legal framework risk, 30% to transaction volume, and 20% to customer type risk to calculate the overall ML/FT risk.
2.3	Custom Hierarchical and Segmented Risk Assessment	• <i>Defining Custom Hierarchies:</i> The System should allow users to define custom risk hierarchies based on the risk levels of clients or services. ◦ Users should be able to classify high-risk clients (e.g., Politically Exposed Persons – PEPs, clients from high-risk jurisdictions) or high-risk services/transactions (e.g., cryptocurrency transactions). ◦ These classifications should be configurable, enabling supervisors to adjust the hierarchy based on emerging threats or changes in regulatory requirements. • <i>Segmented Risk Assessments:</i> The System should support segmented risk assessments for each defined	For example, users can define high-risk clients based on their presence in high-risk jurisdictions or involvement in specific economic sectors (e.g., the gambling industry). For example, the System can group transactions based on client type and jurisdiction, enabling segmented risk assessments for high-risk clients



		group, based on pre-established risk categories. ○ Each segment (e.g., high-risk clients, high-risk products/services) should be evaluated separately, and risk scores shall be calculated based on weighted factors relevant to each risk dimension. ○ The System should allow flexible configuration of these weights and scoring rules, so that supervisors can adjust them as new risks or regulations emerge.	engaged in cross-border transactions. For example, the System can evaluate the risk level of high-risk clients by considering the frequency and volume of transactions, and assigns risk scores based on these criteria.
2.4	Export Functionality for Risk Assessments	• Export Formats: The System should allow users to export inherent risk and control quality assessment results in standard formats including Excel, CSV, PDF, and Word. • Detailed Content: Exported files should include detailed descriptions, calculations, and all relevant model parameters, ensuring traceability and transparency. • Structured Output: The exported files should be clearly structured to support easy documentation, review, and archiving by supervisory staff. • Audit Logging: All export actions should be logged, and export history shall be accessible to System	For example, the System should allow for the export of survey results, risk assessments, and risk classifications for each financial institution (FI).



		administrators for monitoring and audit purposes.	
2.5	Regional Risk Models Built on the Risk Profiles of Individual Jurisdictions or Predefined Jurisdiction Lists, with the Ability to Assign Different Risk Weights to Each Jurisdiction or List	• <i>Individual Jurisdiction Risk Factors:</i> Each country or jurisdiction should be assessed based on at least the following indicators: ◦ Regulatory and legal frameworks ◦ Effectiveness of ML/FT controls ◦ Inclusion on international sanctions or watch lists (e.g., FATF high-risk jurisdictions) ◦ Political stability, level of corruption, and economic transparency • <i>Risk Categorization of Jurisdictions:</i> Jurisdictions may be grouped into risk categories (e.g., high-risk, medium-risk, low-risk) based on defined criteria. • <i>Dynamic Risk Lists:</i> These jurisdictional risk lists should be configurable and subject to updates based on changes in regulatory environments or international status reviews. • <i>Weighted Jurisdiction Scoring:</i> Each jurisdiction or list may be assigned different weights according to its risk profile, influencing overall risk calculations in the System.	• For example, high-risk jurisdictions (e.g., countries known for financial secrecy and weak AML/CFT frameworks) may be assigned higher weights, increasing the significance of transactions linked to those jurisdictions from a ML/FT risk perspective. • Lower-risk jurisdictions may be assigned lower weights.



2.6	Specific Regions (e.g., States or Provinces within a Jurisdiction) with Differentiated Risk Weights	Each specific region within a country may be assigned a distinct risk weight, meaning that certain regions can be considered riskier than others. This is important for risk-based assessments where different states, provinces, or administrative areas within the same country may carry varying levels of risk—based on local laws, regulatory environments, or economic stability.	For example, in the United States, Nevada—due to its liberal business laws—may be assigned a higher risk weight compared to other states.
2.7	Custom Lists (e.g., Currencies) with Variable Risk Weights per Entry	- Custom List Creation: Users should be able to create and define custom lists based on organizational needs (e.g., currencies, assets, transaction types). - Support for High-Risk Categories: These lists may include high-risk currencies, sensitive products, or vulnerable customer groups. - Risk Weights for List Items: Each item in the list (e.g., specific currencies such as USD, EUR, or Bitcoin) may be assigned a specific risk weight, determined according to its assessed risk level.	For example, the supervisor may assign a higher risk weight to cryptocurrencies (e.g., Bitcoin) compared to traditional currencies (e.g., USD or EUR), taking into account their level of anonymity.
2.8	Segmentation of Data Points by Country, Region, or Specific Lists	- The System must allow users to segment transaction-related data by country, displaying the results based on the selected jurisdiction. - The System must support regional filtering and analysis by enabling the analysis of data specific to designated geographical areas.	



2.9	Performance of Risk Assessments (Relative Risk) of Institutions Within the Given Sectors	• The System must first generate risk profiles, taking into account ML/FT vulnerabilities—for example, in the banking and insurance sectors. These profiles are essential to understand how different institutions are exposed to money laundering or terrorist financing risks. • The System must classify institutions based on their risk level, allowing comparison between them. Institutions with high-risk scores (e.g., based on factors such as KYC practices, cross-border transactions, etc.) should be flagged with red indicators for enhanced monitoring and supervisory measures. • The System must identify outliers through comparison based on ML/FT risk factors, revealing institutions with relatively higher or lower risk levels.	
2.10	Ability to Transition from FI-Level Risk Assessments to Sectoral and National Risk Assessments (Absolute Risk)	• The System should assess the absolute ML/FT risk by examining vulnerabilities specific to the sector, such as cross-border transactions, links to high-risk sectors or jurisdictions, or complex ownership structures. It should also consider regulatory weaknesses, such as inadequate implementation of KYC (Know Your Customer) procedures. The risk assessments should be based on specific ML/FT indicators, such as the percentage of high-risk	



		customers or businesses in the sector, the volume of unusual or large transactions that may indicate money laundering risk, failure to report suspicious transactions, or discrepancies in reporting. • The System must automatically process data obtained from financial institutions' risk assessments as key input for sectoral and national risk assessments. • This processing should ensure that sectoral trends and risks identified at the FI level are directly fed into higher-level assessments. • These assessments should provide data that can serve as input for the National Risk Assessment (NRA). • These assessments should support the formulation of policy decisions, resource allocation, and regulatory strategies aimed at mitigating the identified risks.	
2.11	Ability to Enable/Disable Data Points for Inherent Risk and Internal Control Assessment.	• Users must have the ability to enable or disable specific data points within the inherent risk and control/management quality assessment models. The System should allow users to specify which data points should be included in the inherent risk assessment (e.g., transaction volume, jurisdictional risk) and which should not. The same applies to the control/management quality assessment, where only active	For example, the supervisor should be able to assess the customer's inherent risk and determine that transaction volume is no longer relevant for the assessment based on new regulations, and therefore disable that data point.



		control criteria should affect the final score. • Disabled data points should not contribute to the overall risk or control assessment, but they must remain accessible for potential future activation. • Only authorized users (e.g., designated supervisors or administrators) should have access to enable or disable these data points. • The System must enforce role-based access control to ensure that only specific users can change the status of data points. • All changes to the enabled/disabled status of data points must be logged by the System. • The log should include who made the change, when it was made, and the reasons for it. • When a data point is enabled or disabled, the System must recalculate the inherent risk and control scores to immediately reflect the modified configuration. • The System should provide alerts or confirmations for enabling/disabling data points, especially when the change significantly affects the risk or control assessment outcome.	
2.12	Assessment Algorithm that Automatically Adapts to	• The assessment algorithm must automatically adjust risk evaluations when variables, hierarchies,	



	Changes in Risk Models	configurations, weights, thresholds, or response ratings are modified. • Changes to the risk model must be reflected in real time, without the need for manual recalculation. • The System must maintain accuracy and efficiency in all recalculations.	
2.13	Enhancing ML/FT Risk Detection through Machine Learning.	• The System should be able to integrate machine learning and artificial intelligence (AI) to independently learn from historical data and improve the accuracy of risk prediction. With System enhancements, it should be able to incorporate predictive analytics—not only to understand current risks but also to forecast future risks based on past data and trends.	For example, the System should be able to identify a trend where a mid-sized commercial bank significantly increases its exposure to high-risk sectors (e.g., real estate, gambling, cryptocurrency exchanges) without a corresponding adjustment to its ML/FT risk management framework or internal controls. Additionally, the bank's suspicious transaction reporting rate declines, despite the rise in transactional volume and customer onboarding. Based on comparative



			analysis with peer banks and historical supervisory assessments, the System should flag the institution for increased supervisory attention, suggesting potential deficiencies in its risk-based approach and possible underreporting of suspicious activity.
2.14	Multiple Financial Sectors and Multiple Institutions within Each Sector.	- The System should be designed to support multiple sectors, such as banking, credit, and insurance, and can be easily scaled to include any number of additional sectors. - It should be able to manage and organize any number of financial institutions within each sector.	For example, models for banks, credit organizations, and insurance companies.
2.15	Building New Risk Models or Customizing Existing Ones	- The System should allow users to create new risk models based on specific parameters such as geography or regulatory requirements. - The System should be able to integrate existing risk models, ensuring a smooth transition or upgrade without losing previously developed frameworks or methodologies. - Users should be able to customize the models based on new data or	



		evolving risk assessment needs, ensuring that risk management processes remain up to date and scalable.	
2.16	Ability to Update Incorrect Data Points	• The System must allow users to identify data points that may be incorrect. • Users should be able to select those data points for correction. • Only authorized users (e.g., administrators or data managers) should have the ability to update data points.	For example, a user who identifies an incorrect data entry in the System should be able to submit a request to the authorized person for the update.
2.17	Roles and Permissions	• The System must include a role and permission management function that allows precise definition, management, and control of user access to various modules and actions, in accordance with the principles of RBAC (Role-Based Access Control), SOD (Segregation of Duties), and Least Privilege. • The System must support a four-eyes approval process for all re-entries related to changes in inherent risk and control/management quality. • All re-entries and actions must be documented in audit logs with clear details on who initiated and approved the actions, as well as system errors and events to support future auditing and debugging.	
3	<u>Data Analysis Capabilities</u>		



3.1	Aggregated Statistical Data for Financial Institutions and Sectors	• The System must provide automatic calculation and aggregation of key AML/CFT indicators across sectors. It should compute, at a minimum, the minimum, average, mode, maximum values, total amounts, and the number of reporting financial institutions, enabling the assessment of sectoral risks. • The System must also provide summaries for each financial institution, allowing the identification of unusual activity related to AML/CFT compliance. These summaries should be available per institution to assess their risk level and the effectiveness of their control/management quality.	For example, it should provide a detailed report on suspicious transactions for a specific bank and compare its values with the sector's average indicators.
3.2	Changes from the Previous Reporting Period, Data Trend Analysis	• The System must detect and record changes between current and previous reporting cycles. These changes may include: ◦ Differences in indicators, both quantitative and qualitative (e.g., increases or decreases in scores) ◦ Changes in risk assessments, thresholds, or other performance indicators ◦ Differences in responses to specific questions or surveys ◦ Institution-specific changes, such as transaction volumes or compliance levels	Example: If a financial institution's risk rating has decreased compared to the previous cycle, the System must highlight the change and quantify the difference. Example: A user may wish to compare only high-risk ratings between reporting cycles.



		• Users must be able to view these changes through comparative reports or dashboards. • The System must support trend analysis for any defined data metric (e.g., risk scores, transaction volumes, compliance violations) over a selected time period. • The System must generate visual representations of metric changes, including line charts, bar charts, or other suitable visualizations. • Metric selection: Users must be able to select which metrics to analyze, and the System should allow comparisons between different metrics. • The System must support both predefined metrics (e.g., risk ratings, transaction volume) and user-defined metrics. • Timeframe customization: Users must be able to select the analysis period—daily, weekly, monthly, quarterly, or yearly comparisons. • Trend analysis indicators: The System must calculate key indicators for trend analysis, including: ◦ Percentage changes over time ◦ Moving averages to smooth short-term fluctuations ◦ Rate of increase or decrease ◦ Detection of peaks and troughs in the data • Visual and tabular reports: The System must generate both visual	Example: A bank may use trend analysis to observe the increase in high-risk transactions over the past six months to detect AML/CFT risks. Example: A financial institution may monitor trends in large cash deposits on a monthly, quarterly, or other time basis. Example: The System should show that the peak in high-value transactions occurred in the first quarter of the year.
--	--	--	--



		reports (e.g., graphs, charts) and tabular reports showing data values over time. • Users must be able to export these reports in various formats, such as Excel, PDF, or CSV. • Anomaly detection or early warning: The System must include an anomaly detection feature to notify users when deviations or unexpected changes are observed in a given metric.	
3.4	Threshold Definition	• The System must support the selection, storage, and application of thresholds for key ML/FT risk indicators. • Users must be able to define and reuse customized AML/CFT thresholds. • The System must automatically generate alerts when thresholds are breached.	
3.5	Dashboards on Sector-Specific and Sector Summary Statistical Data	<i>Sector Summary (Including Statistical) Dashboards:</i> • These dashboards should provide a comprehensive view of overall risk factors and trends within a given sector. Users should be able to access key data insights. • They should highlight regulatory compliance, emerging risks, or opportunities for improvement. • They should deliver summary statistical data, such as overall risk levels within the sector.	For example, in the financial services sector, the regulatory authority can use aggregated statistics—based on data received from banks—to assess the overall sectoral risk level, such as AML/CFT and sanctions compliance risks, or



		• This information should be presented in visual formats (charts, tables, or graphs) to simplify data interpretation and facilitate understanding of complex datasets. • Summary dashboards should allow users to compare performance across different financial institutions or sectors, helping identify patterns or deviations. <i>Customizable Views:</i> • Supervisors should be able to frequently personalize the dashboards to focus on specific metrics, timeframes, or areas of interest. <i>Real-Time Data:</i> • These dashboards typically display real-time or near real-time data, enabling quick responses to changes in sector performance or risk levels.	their recent increase.
3.6	Horizontal Comparison of Ratings, Responses, and Rankings Across Multiple Financial Institutions.	• The System should display data from multiple financial institutions side by side, making it easier to compare their risk scores or survey responses across different categories or criteria. • The comparison should include ratings (e.g., risk scores, compliance ratings), responses from surveys or assessments, and rankings, allowing users to see which institution	Example: Banking sector: The regulatory authority should be able to compare the risk ratings of different banks side by side to understand which institutions are the most effective in risk management.



		performs best or worst in each category. • Users should be able to customize the criteria or indicators being compared to align with their operations or regulatory requirements. • The System should allow users to filter and sort results, focusing on specific sectors, timeframes, or types of responses. • Comparisons should be frequently presented in visual formats (charts, tables, graphs), enabling users to quickly identify patterns or deviations across institutions.	
--	--	---	--

ARCHITECTURAL REQUIREMENTS

No.	Requirements	Description
1.	Operating System: Windows Server 2019 or later is preferred	It is desirable for the System to run smoothly on Windows Server 2019 or later versions. The System must not use outdated or vulnerable protocols (e.g., SMBv1, TLS 1.0/1.1).
2.	Database Requirement: Preferably DBMS or MS SQL Server	The System must be connected to at least one of the following databases: DBMS, MS SQL Server, Oracle, PostgreSQL, or MySQL-MariaDB (It is preferable that the System support the latest long-term support (LTS) version to avoid outdated and vulnerable releases.)



		These databases are compatible with all major web browsers (See Chapter 9, Point 3).
3.	Integrated with a flexible monitoring system	A flexible monitoring system with filtering capabilities (including monitoring of specific components, such as workflow monitoring) to minimize the time spent on detecting and resolving failures, identifying root causes, and filtering incident-related notifications.
4.	System recovery tools	In case of necessary access, users must be able to recover any lost system information. The System must be integrated with Veeam software.
5.	System management tools	System management tools should be fully accessible (user registration, assigning user permissions, user replacement, directory maintenance).
6.	System performance assurance tools	System performance assurance tools should be provided by the Bidder.
7.	Integration capabilities	Integration capabilities should include the use of any of the following architectures: Client/Server, N-tier, middleware architecture, and service-oriented architecture (SOA).

REQUIRED FUNCTIONS FOR SYSTEM ADMINISTRATION, INTEGRATION, AND MANAGEMENT

No	Requirement	Description	Example
----	-------------	-------------	---------



1.	The software should enable the segregation of user access rights/roles.	(a) User access roles/permissions are entered into the System for the purpose of user and role management. (b) The specified information can be entered into the System either manually or through automated queries from other systems (e.g., AD, SSO, etc.). (c) Successful registration of users implies configuration of all applicable permissions/roles, assignment to the relevant branch of the organizational structure, and identification of the user performing actions or changes in the System (principle of non-repudiation).	Example: A new supervisor receives access from Active Directory (AD) to general and function-specific processes in accordance with his/her responsibilities.
2.	All user actions within the System must be logged.	Ability to log user actions within the process. Specifically: 1. The System must retain logs of all user	



		login and registration activities to support security monitoring and anomaly detection. 2. The System must enforce a Password Policy to ensure the use of strong and regularly updated passwords.	
3.	The System should maintain an audit log of all file exports.	(a) The audit log must include export activities, including the user who performed the export, and the date and time of the export. (b) Files exported from the System must contain sufficient information to identify the exporting user. If any such information is modified, the file must become invalid/corrupted. (c) The System must support integration with the Trellix SIEM solution for security information and event management, enabling monitoring of file exports, detection of anomalies, and	Example: If a user downloads a file from the System, a unique signature or the user's full name is attached to the file.



		prevention of unauthorized modifications.	
4.	The System should provides functional capability for event log management.	(a) Functional capability for logging and monitoring predefined System events (including errors and limitations encountered during operation). (b) Error categorization and assignment to different administrator groups.	Example: Separation of service integration errors from database access errors and assignment to different administrator groups.
5.	The System should include management and monitoring window.	Real-time display of System performance and availability information.	Example: Real-time graphical representation of performance and errors.
6.	The System must support the following technologies/protocols for integration with external systems.	The System must provide diverse mechanisms for data transmission and integration, which are essential for reliable, secure, and efficient interoperability between different systems. Below are the key technological requirements for data exchange: • API protocols (REST, SOAP, RPC) • FTP/SFTP • Direct access to databases using any technology	



		• MQ technologies	
7.	The system must support the following data exchange formats	XLSX, CSV, JSON, XML, or other widely accepted standards.	

SYSTEM PERFORMANCE AND USER INTERFACE REQUIREMENTS

No.	Requirements	Description
1.	Ensuring fast and uninterrupted service for at least 10 users simultaneously (maximum capacity: 50 users).	Uninterrupted operation and System accessibility for concurrently active users.
2.	The System should be scalable to efficiently process large-volume files without any deterioration in performance.	The System should be capable of handling increasing volumes of data without affecting its speed or reliability. It must incorporate monitoring mechanisms and utilize caching and compression techniques to ensure that working with large files does not impact System performance.
3.	The System should be browser-independent and accessible to users across various devices and platforms.	Multi-browser compatibility: The System should be compatible with all major web browsers, including Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari, and others.
4.	The System should be capable of supporting the assessment of a large number of sectors and	The System should support the assessment of at least the following sectors and corresponding financial institutions on a monthly basis: banking, credit, payment and settlement, and investment



	financial institutions at least on a monthly basis.	organizations (including the depository). Specifically, this includes 17 banks, 42 credit organizations, 16 payment and settlement organizations, 22 investment companies, and 1 depository. The System should also be designed to allow for increasing the assessment frequency to near-real-time or real-time in the future, which is preferred.
5.	The System should be user-friendly and easy to navigate for all users.	• Easy and Intuitive Navigation – The System structure should allow users to quickly find the required functionality without extensive searching. • User Journey Clarity – The UI/UX design should ensure that users clearly understand their next steps and can easily perform the required actions. • Accessibility – The System should be suitable for a wide range of users and preferably be compliant with the Web Content Accessibility Guidelines (WCAG) 2.1. UI/UX Evaluation – The usability of the System (UI/UX) should be evaluated by a designated committee that will assess the design’s convenience, clarity, and effectiveness in order to enhance the end-user experience.

SYSTEM SECURITY REQUIREMENTS

No.	Requirement	Description	Example
1.	The System should ensure the security of data	The System should ensure secure data transmission between the user and the server, preventing data	



	exchange between the user and the server.	leakage, unauthorized access, and cyber threats.	
2.	Compliance with international security standards	The System should preferably comply with international security standards, such as ISO 27001 – Information Security Management System. Specifically, the System should comply with at least the following controls of the ISO/IEC 27001:2022 standard: • 8.25 – Secure development life cycle • 8.26 – Application security requirements • 8.27 – Secure System architecture and engineering principles • 8.28 – Secure coding • 8.29 – Security testing in development and acceptance • 8.30 – Outsourced development	
3.	The System should provide the ability to set limitations on attachments, including size, format, and other relevant criteria.	The System should provide an attachment restriction functionality, enabling control over file size, format, and other parameters in accordance with information security and data management requirements.	
4.	System Disaster Recovery Plan	The System should ensure automatic backup, data recovery, uninterrupted operation during emergency	



		situations, and rapid restart mechanisms (Failover & Failback). It should also comply with the defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) criteria.	
5.	The System should have functional capabilities to parse, encrypt, and decrypt files.	• The System should provide functional capabilities for encrypting, decrypting, and parsing files using encryption keys. Modern encryption algorithms (such as AES) shall be applied, and key management should be performed through a Key Management System (KMS). The System should also support the automated execution of encryption and decryption processes. • The System should ensure that all sensitive data is encrypted both in transit and at rest, using at least SHA-256 (Secure Hash Algorithm 256-bit). This encryption standard prevents unauthorized access to data, even if it is intercepted or compromised.	



6.	Security Authentication and	• Multi-Factor Authentication (MFA): The System should implement MFA, requiring users to provide two or more authentication factors to access the System (e.g., a password plus a one-time code (OTP) delivered via email or SMS). • Integration with Advanced MFA Solutions: The System should integrate with MFA solutions that support user authentication through mobile applications, including Push Notification mechanisms and OTP-based authentication. Accepted solutions include (but are not limited to) Openspan, Thales, or other industry-compliant platforms that meet security standards. • Role-Based Access Control (RBAC): The System should enforce role-based access control to restrict access to data and System functionalities based on the user's assigned role. This minimizes the risk of unauthorized access and data misuse. • User Activity Logging and Monitoring: The System should maintain comprehensive logs of user activities, including login	
----	-----------------------------	--	--



		attempts, data modifications, and other critical actions. This enables the detection of suspicious behavior and potential security violations. • Integration with Trellix SIEM (Security Information and Event Management): The System should integrate with Trellix SIEM to automatically and continuously forward all relevant events, actions, and security logs for centralized monitoring and incident detection.	
7.	Business Continuity	• Redundancy: The System should support redundancy across key components (e.g., servers, databases, storage) to eliminate single points of failure. In the event of a component failure, the redundant counterpart should automatically take over to ensure uninterrupted service. • Monitoring and Alerts: The System should include proactive monitoring and alerting mechanisms to help administrators detect and respond to potential issues before they cause disruptions. This functionality supports	



		continuous availability and operational reliability.	
--	--	--	--

AUDITABLE REQUIREMENTS

No.	Requirement	Description
1.	Unsuccessful login attempts	• The System should restrict the number of consecutive invalid login attempts by a user. • In case the maximum number of unsuccessful login attempts is exceeded, the System should either automatically delay the next login prompt in accordance with system configurations or lock the account until it is manually unlocked by an administrator. Additionally, a notification mechanism should be in place to alert relevant personnel when the threshold for failed login attempts is exceeded.
2.	Session termination	• The System should automatically terminate a user session after a defined period of inactivity.
3.	Automated labeling	• The System should use standardized labeling templates to tag outgoing data in order to identify any special instructions for dissemination, processing, or distribution.
4.	Auditable Events	The System should generate audit logs for the following events: • Creation, activation, modification, review, deactivation, and deletion of user accounts • Creation and modification of protected objects, and access to them • Login and logout events • Unsuccessful login and access attempts



5.	Audit Content Log	• The System should provide audit logs that contain sufficient information about the events that occurred, their sources, and the outcomes of those events. The content of audit logs shall include: ○ Date and time of the event ○ System component involved ○ Type of event ○ Identity of the user/entity ○ Outcome/result of the event (success or failure) • The System should allow the inclusion of additional, more detailed information in audit logs based on event type, location, or entity involved. • The System should enable centralized management of the content of audit logs generated by individual components across the entire System.
6.	Response to Audit Process Failures	• In the event of audit process failures, the System should notify the relevant authorized personnel within the organization. • Audit process failures may include, for example: software/hardware errors, failures in the audit logging mechanism, and exceeding or exhausting audit storage capacity • The System should issue a warning when the allocated storage for audit logs approaches a defined threshold.
7.	Audit Reduction Log and Report Generation	• The System should provide the capability to reduce the volume of audit logs and generate reports • The System should support the automated processing of audit records related to events of interest, based on configurable event criteria.



8.	Protection of Audit Information	The System should ensure the protection of audit information and audit tools from unauthorized access, modification, and deletion.
9.	Non-repudiation	The System should provide the ability to determine whether a specific individual has performed a particular action.
10.	Minimum Functionality	The System should provide the ability to configure only essential capabilities, and explicitly disable and/or restrict the use of all non-essential functionalities, interfaces, protocols, and/or services.
11.	Transmission Integrity	The System should protect the integrity of transmitted information. It shall should cryptographic mechanisms to detect any modifications during transmission, unless the information is safeguarded by alternative physical means.
12.	Transmission Confidentiality	The System should protect the confidentiality of transmitted information. To prevent unauthorized disclosure during transmission, the System should employ cryptographic mechanisms unless the information is secured by alternative physical means.
13.	Data Confidentiality and Protection	The Vendor should ensure the strict confidentiality, integrity, and security of all information shared or accessed in connection with the Contract, including but not limited to regulatory reports, supervisory inquiries, ML/FT and sanctions compliance risks assessments, and any other sensitive or proprietary data. - The Vendor is strictly prohibited from disclosing, processing, transferring, copying, or otherwise using any real supervisory data for testing or development purposes. - For system testing, only anonymized and artificial (“dummy”) data, generated or approved by the Client, shall be used.



		• Should on-site testing be required, the Vendor's authorized representative must be physically present at the Client's premises and under direct supervision of authorized personnel. • Any unauthorized access, disclosure, processing, or misuse of data shall constitute a material breach of contract, subject to immediate termination and legal liability in accordance with applicable laws and regulations. • The Vendor shall be required to sign a Data Confidentiality and Non-Disclosure Agreement (NDA) prior to any access to the system environment.
14.	Security Testing and Risk Assessment	• The vendor must conduct annual penetration testing and vulnerability assessments to ensure the AML/CFT System remains secure. Upon request, the vendor is obligated to provide detailed security testing reports. It is preferable that the System is protected against vulnerabilities listed in OWASP Top 10 and SANS/CWE Top 25.
15.	Data Deletion	• Upon contract termination or in accordance with data retention policies established by law, all stored data must be securely deleted using industry-accepted data wiping technologies. Methods that ensure data irrecoverability shall be applied, such as DoD 5220.22-M and NIST 800-88 standards.
16.	Accuracy, Completeness, Validity, and Authenticity of Information	• The System should verify the accuracy, completeness, validity, and authenticity of information.



17.	System Component Inventory	• Inventory and Information on Ownership: The participant shall develop and provide an up-to-date inventory of all System components, including relevant documentation regarding their ownership status. • Use of Open-Source Software: According to policy, the use of open-source software is not recommended unless it meets the required security and support standards. • Support for Third-Party Software: Any third-party software components used within the System must be up to date and supported. The use of outdated or unsupported software is strictly prohibited.
18.	System Recovery and Reconfiguration	• The applicant shall provide mechanisms, supported by auxiliary procedures, to restore and reconfigure the System to a known secure state following a failure or malfunction. The complete System restoration and reconfiguration shall be included as part of disaster recovery plan testing.
19.	System Maintenance Policy and Procedures	• The applicant shall develop and provide: (i) a formal, documented System maintenance policy outlining its purpose, scope, and roles, and (ii) formal, documented procedures to ensure the implementation of the System maintenance policy and related System maintenance controls.
20.	Timely Maintenance	• The applicant shall provide maintenance and support for an agreed-upon period.
21.	System Documentation	• The applicant shall provide authorized personnel with appropriate documentation related to the System. The documentation shall include administrator and user guides containing information on: (i) System configuration,



		deployment, and operation; and (ii) effective use of the System's security features.
22.	Configuration and Change Management	• The Vendor shall demonstrate that the proposed off-the-shelf solution is managed under a formal configuration and change management process, including secure updates, documented change logs, and communication of major changes or patches to the Client.
23.	Third-Party License	• If the implementation of the proposed solution requires the acquisition or use of a third-party license, the Central Bank shall bear no obligation to accept the applicant's proposal in that regard or assume any related legal, financial, or technical responsibilities.

GENERAL TECHNICAL REQUIREMENTS

No.	Requirement	Description
1.	The programming code used in the System shall be based on the latest available versions.	• The System's source code, databases, and programming frameworks must utilize the latest available stable versions. • All System components must currently be supported by their respective vendors. • Discontinued or obsolete technologies must not be used. ○ The use of software that has reached End of Life (EOL) or End of Support (EOS), as officially declared by the vendor or development group, is strictly prohibited. ○ Software not receiving security updates must be replaced or updated with appropriate alternatives. • All utilized software must ensure full compatibility with other System components.



		• Third-party software must be backed by long-term support (LTS) guarantees.
2.	The vendor shall submit a System implementation plan.	• The implementation plan shall include, at a minimum, the following: ○ A schematic diagram of the System components' integration and installation ○ A description of network connections ○ A description of data flows ○ Configuration files and their descriptions ○ A list and description of third-party/vendor-provided resource components and their required capacities necessary for System maintenance and operational continuity
3.	The vendor, with the participation of the client's specialists, shall configure the "Testing Environment" and "Production Environment."	

TRAINING AND EDUCATIONAL MATERIALS

N o .	Requirement	Description
1.	The Vendor shall provide all necessary user guides and	• User manual: A detailed user manual must be provided, explaining the core functionality of the System. It should



reference materials to ensure effective use of all System components.	include step-by-step instructions, navigation guides, and troubleshooting tips. • Risk modeling guidelines: A dedicated risk modeling guide must be provided, outlining how the System calculates risks, how to define risk parameters, and how to interpret risk assessments. • Training program: A training program must be provided alongside the System, detailing course topics and materials, covering both basic user training and advanced risk modeling techniques. • First-line support guidelines: A first-line support guide must be provided, including general troubleshooting steps and processes, including: ○ Basics of System error resolution ○ Frequently asked questions (FAQ) and answers to common user issues ○ Instructions on escalating issues to higher-level support • Technical operation manual: A manual for System operators and administrators, including regular maintenance schedules, data archiving, recovery mechanisms, backup replication, troubleshooting, and more. • API definitions: A complete API specification package must be made available to assist developers in integrating the software solution/platform with other systems. This should include: ○ A comprehensive list of API endpoints ○ Authentication protocols and mechanisms ○ Definitions of input/output data formats ○ Sample requests and responses ○ Rate limiting and error handling policy
---	---



		○ Technical limitations
2.	System Administrator Guide	• The purpose of the program (or System) and its scope of application, • The structure of the program, its operational principles, • The delivery package (if not specified in a separate document), • The System requirements for the program or its components, • The preferred installation sequence of the components, • The installation process for the program or each of its components, • The mandatory configuration sequence for the program, • The integration methods for the installed copies of the components, • The integration of the program, e.g., with software, database server, • Methods and frequency of verifying the accuracy of program operation, • The current maintenance procedure for the active program copies, • The process for resolving any potential support issues, • Emergency situations and the methods for overcoming them, • User interface for the administrative panel, • Command-line interface tools and their execution sequence, • Configuration files and their writing rules, • The scripting language for writing control scripts.
3.	User/Technical Team Training	The vendor shall conduct initial training sessions prior to the implementation of the System to prepare staff for smooth operation of the System. Specifically, the technical team



		shall receive training in, at least System deployment, APIs, replication, and maintenance, while the AML/CFT team shall be trained in at least risk models, preventive Systems, dashboards, and reporting. It is also desirable to conduct training sessions for business analysts and management.
4.	The training sessions shall be conducted annually by the service provider, as required by the Central Bank.	The vendor (service provider) shall conduct annual training sessions focused on the effective use of the System, ensuring security, and adopting new features, as per the Client's requirements.

TESTING/VALIDATION

No.	Requirement	
1.	Deployment validation	The Vendor shall: • Provide all relevant documentation (see Chapter 13 for details), including the deployment verification checklist, configuration, and integration documentation. The Client shall: • Perform system configuration based on the documentation provided by the Vendor, in alignment with supervisory business logic and risk methodology. • Confirm that network and integration points are functioning as intended. • Review and approve the submitted documentation.



		- Formally confirm readiness to proceed to acceptance testing only after successful deployment validation. Deployment validation is considered successful (pass) if: - All system components are operational and accessible. - Information security and integration are verified. - Configuration aligns with supervisory requirements. - No outstanding technical issues remain. - All required documentation is submitted and approved by the Client.
2.	Acceptance Testing (QA + UAT) — In Line with ISO/IEC 12207 and ISO/IEC 90003	The Vendor shall submit a testing plan, including a test guide and acceptance criteria, enabling the evaluation of whether the deployed system meets the Client’s business, functional, performance, security, and usability requirements, based on real supervisory scenarios and test cases. Vendor Responsibilities - Support the Client throughout the testing phase by: - Assisting in the logging and classification of defects - Ensuring timely resolution of bugs and correction of defects - Track all issues in a defect Log, including status, severity, resolution date, and retesting outcome. - Upon completion of testing, provide a summary report covering test coverage and identified issues. Client Responsibilities - Provide a fully operational test environment aligned with the production configuration. - Execute test scenarios that reflect real supervisory use cases (e.g., risk scoring validation). - Review outputs such as dashboards, alerts/red flags, and reports for accuracy and compliance.



		- Log all results and defects using the pre-agreed classification methodology (e.g., Critical, High, Medium, Low). - Validate key non-functional aspects, including system performance, authorized access, and usability. - Confirm whether each requirement has been met based on predefined acceptance criteria (e.g., expected scores, accuracy of workflows, compliance of reports). Testing is considered "Accepted" (pass) if: - All business scenarios operate fully and correctly without errors or defects. - No unresolved bugs or deficiencies remain. - Value attributes such as functionality, performance, usability, security, and integration are confirmed. - All test documentation, defect logs, and resolution reports are reviewed and approved by the Client.
3.	Defect classification and resolution during acceptance testing (QA + UAT)	Each defect logged during acceptance testing must be classified by severity: - Critical – Blocks essential System functionality (e.g., incorrect risk scoring, failed data import) - High – Impacts core business workflows (e.g., incorrect escalation of alerts/red flags, non-functional dashboards) - Medium / Low – Non-blocking user interface bugs or improvement suggestions Defect resolution: The Vendor is responsible for: - Applying technical fixes - Optimizing configurations and parameters - Updating APIs or integration components as needed Retesting and closure process



		• After fixes are deployed, the Client must retest the failed scenario(s) to confirm the issue has been resolved. • Closure is permitted only after the Client confirms resolution and successful retest results are documented. The defect resolution phase is considered successfully completed (Passed) when: • All defects are closed and approved by the Client • No new issues have emerged during retesting • All defects and resolutions are fully documented • The updated Defect Log is approved by the Client
4.	Pilot run	The pilot phase should focus on validating the operational supervisory workflows using real data. The following key components are typically included: • Risk scoring logic and alert thresholds • Generation of red flags and supervisory dashboards • Visualization and report generation The purpose of the pilot is not to exhaustively test all system functionalities, but rather to ensure that the core supervisory logic functions correctly and that users can perform their essential tasks effectively. The Pilot Phase is considered successful (“Accepted”) if: • Supervisory users are able to complete end-to-end workflows without obstacles or failures • No logic errors or system crashes occur during run • Users confirm that key value attributes (e.g., functionality, usability, risk scoring, navigation) are satisfactorily met
5.	Go-Live Readiness Sign-Off	The following phases must be fully completed and approved before Go-Live Readiness can be confirmed:



		• Deployment Validation ▪ All system modules are deployed, configured, and accessible • User Acceptance Testing (QA + UAT) ▪ All functional and non-functional requirements are verified • Defect Resolution ▪ All issues are resolved and closed • Pilot Run ▪ Critical/core workflows are demonstrated by real end-users • Training Completion (<i>see Chapter 13 for details</i>) ▪ End-user training conducted for supervisors, analysts, and administrators • Documentation Delivered ▪ Technical architecture, configuration summaries, user manuals, and standard operating procedures (SOPs) Pass Condition: The Client signs the Go-Live Readiness Certificate, confirming that the solution meets all operational criteria and is ready for production use. Fail Condition: Unresolved defects, missing documentation, or open testing gaps prevent the system from going live.
--	--	---

TECHNICAL SUPPORT REQUIREMENTS

No.	Requirement	Description
-----	-------------	-------------



1.	Within the scope of the vendor's support, the vendor shall provide System maintenance for an average period of 5 years.	• Technical Support and Maintenance • System Updates and Optimization • Security Support • User Support and Training • Periodic Reporting and SLA (Service Level Agreement) Compliance: The SLA should include specific response times (e.g., confirmed deadlines for error resolution during the warranty period).
2.	The complete and full source code, along with the accompanying detailed documentation, shall be provided by the Vendor to the Client, including any relevant tools and utilities, if available, that are required for modifying, reconfiguring, deploying, testing, and transferring the application to the production environment.	• The Client shall be provided with the complete and modifiable source code (including dependencies and configurations), allowing for future software modifications, installation, and adaptation. • The Vendor shall supply all necessary accompanying documentation to enable the technical team to fully understand and manage the System.
3.	Technical support shall be available at three levels.	• First Level (Internal Support provided by the Client): Adequate training, along with all necessary source code and documentation, must be provided to enable the Client's IT personnel to offer first-level support for System operation and resolve issues raised by participants and customers. • Second Level (Remote Support provided by the Vendor): The Vendor shall provide necessary support and maintenance through remote



		communication methods such as remote access, email, phone, and remote desktop software. • Third Level (On-site Support provided by the Vendor): The Vendor shall be available in Armenia within reasonable timeframes and provide rapid expert support. Any time and expenses incurred for such support should be included in the financial proposal.
4.	Warranty and Operational Support	• The Vendor shall provide a warranty for all solution components delivered within the specified warranty period, which shall be at least equal to or longer than the warranty period provided by any subcontractor. • During the specified warranty period, the Vendor shall act as the Client's agent for requesting repairs or corrections for any component supplied and guaranteed by the vendor. The components under warranty shall be repaired without any additional charge to the Client. • The warranty for the application software shall be effective for one year from the official acceptance date, as recorded at the completion of acceptance testing. • During the warranty period, the Vendor shall, if necessary, provide on-site operational support by sending at least one expert from the Vendor's team (who directly participated in the software deployment) to assist the Client's operational team.
5.	Technical Support	• The Client shall receive consultancy on new features related to the development environment, supporting resources, and related technological



		requirements to ensure that the Client possesses the complete and appropriate set of tools and capabilities necessary to guarantee the reliable and continuous operation of the System. • The Vendor shall provide Second-Level Technical Support, which will be available for at least five (5) calendar years starting from the day after the warranty period ends. During the technical support period, the Vendor shall make best efforts to assist the Client in achieving software stabilization (bug fixes, troubleshooting), issue identification and resolution, and provide relevant knowledge, capabilities, and expertise in the technical support domain, if necessary. The Vendor shall perform on-site inspections and preventive maintenance at the Client's request, for which the Client will incur costs. • During the support period, the Vendor agrees to provide Third-Level Technical Support upon the Client's request.
6.	Documentation Updates	• All detailed technical specifications, including all updates, additions, and other modifications, shall be provided to the Client before implementing any such update, addition, or modification in the test or production environment. • All accepted international and industry standards, as well as applicable local standards, must be clearly referenced and accompanied by detailed descriptions of similar standards.



		• Detailed and up-to-date documentation may also be provided in Armenian. • The Vendor's local technical support agent, if applicable, must be informed and thoroughly familiar with the technical documentation available to the Client, as well as the hardware and software environment of the System.
--	--	---



SYSTEM PRESENTATION REQUIREMENTS FOR THE STAKEHOLDER

The applicant must also ensure the complete presentation of the System through a stakeholder presentation.

TIMELINE PROJECTIONS

The implementation deadline for the present project shall be six (6) months from the date of contract signing, with the possibility of extension upon mutual agreement of the parties. The participant shall provide a detailed timeline in the proposal, at a minimum including the expected outcomes listed below.

EXPECTED OUTCOMES
System Implementation Timeline (by each process)
Project Execution
Training Schedule
Final Acceptance Delivery
Warranty Support

The Vendor shall provide the Project Management Plan and the Project Implementation Timeline. If necessary, the Vendor must be physically present during the System deployment, acceptance testing, handover-acceptance, and training phases.

EVALUATION AND QUALIFICATION

1. QUALIFICATION CRITERIA FOR PARTICIPANTS

In addition to being eligible to participate, the Participant must meet the following minimum qualification requirements.

- 1.1. At least 3 years of experience in automating ML/TF and sanctions compliance risk assessments and implementing advanced supervisory technology (SupTech) solutions, operating as a registered company/entity. Demonstrated successful implementation of similar systems in other regulatory authorities, aligned with the required standards (e.g., FATF 40 Recommendations).



As evidence, the organization shall submit its portfolio, including information on properly implemented systems within the three years prior to submission of the application, detailing the client's industry, implementation timeline, and scope.

The Participant shall also provide reference letters from previous clients confirming that provided systems were successfully implemented, are operational, and meet the required standards.

- 1.2. The Participant must allocate qualified personnel to carry out the required tasks and ensure the achievement of the Contract objectives in terms of both timeline and quality. The personnel involved in the implementation of the project must possess the necessary qualifications, a minimum of five (5) years of professional experience, and demonstrated skills in executing similar projects, ensuring high-quality performance. The Participant shall provide a team of experts with expertise in AML/CFT compliance, regulatory reporting, software integration, cybersecurity, and system support.

As evidence, the Participant must submit the CVs of key experts (including supporting documentation confirming their qualifications), clearly indicating their relevant work experience and number of years in each role. All team members must have at least working proficiency in English (knowledge of Russian is desirable).

2. APPLICATION SUBMISSION REQUIREMENTS

2.1. Financial/Price Proposal

- 2.1.1. The financial proposal must include the total cost for the System implementation, as well as the anticipated post-implementation expenses over a five-year period. This includes the costs of implementation, deployment, operation, training, maintenance, support, travel to the Republic of Armenia (if required), and any other necessary expenditures (in accordance with Annex 3, which is the sum of Annex 3.1 and Annex 3.2).
- 2.1.2. The Participant shall submit a detailed breakdown of the System implementation costs using Annex 3.1, clearly specifying the unit and total prices for each proposed component.



- 2.1.3. The Participant shall provide a separate breakdown (using Annex 3.2) of the expected post-implementation costs over a five-year period, including post-warranty maintenance, support, and other required expenses. This must take into account at least one year of warranty service, as well as clearly outline the payment terms, schedule, and procedures.
- 2.1.4. The Participant may also submit additional optional proposals, if any, which may be considered at the sole discretion of the Client.

2.2. Technical Proposal

- 2.2.1. As part of the application, the Participant shall submit a detailed description of the proposed System, including the following:
 - 2.2.1.1. A Technical Proposal that meets the requirements specified in the Technical Terms of Reference, including compliance with international security standards, usability features such as ease of use, simplicity of administration and further development, compatibility with existing infrastructure, and any other relevant information.
 - 2.2.1.2. Warranty and post-warranty support terms for the System.
 - 2.2.1.3. Implementation roadmap and detailed timeline provided by the Participant.
 - 2.2.1.4. Training methodology, schedule, and other necessary arrangements.
 - 2.2.1.5. Any other information the Participant deems appropriate to best present and describe their proposal.
 - 2.2.1.6. For software solutions, a Manufacturer's Authorization Form (MAF) must be submitted, issued either by the original software producer or its official representative, confirming authorization to supply the product in the Republic of Armenia.
 - 2.2.1.7. Information on the existence of a certified service center in Armenia authorized by the manufacturer, or confirmation that the manufacturer provides servicing through a centralized service center. The details of such service centers must be available on the manufacturer's official website or validated by appropriate certificates.
 - 2.2.1.8. Information on the warranty period and System recovery time.
 - 2.2.1.9. The company's registration certificate.
 - 2.2.1.10. Documentation on professional experience in accordance with Annex 5 of this Invitation.
 - 2.2.1.11. Documentation confirming the availability of necessary human resources in accordance with Annex 6 of this Invitation.
 - 2.2.1.12. Certificates of compliance with international information and cybersecurity standards (e.g., ISO 27001).

3. PROPOSAL EVALUATION



During the evaluation of proposals, both price and non-price criteria will be taken into account. In this methodology, the weight of **non-price criteria and the Technical Proposal is 70%, while the weight of the Price Proposal is 30%**. The contract will be awarded to the Participant with the highest combined score based on both price and non-price criteria.

Only the price proposals of those Participants whose Technical Proposal scores at least 70 out of 100 points will be considered for comparison. The overall technical score (TS) represents the weighted combined score of all evaluated technical characteristics.

Evaluation Criteria	Weight (%)	Maximum Score
Technical Proposal Evaluation	70	
Alignment with Regulatory Standards, Functional Suitability, and Degree of Innovation of the Proposed Solution		30
• Technological solution and compliance with international AML/CFT frameworks (e.g., FATF)		20
• User Interface (UI/UX) accessibility, intuitive navigation, and dashboard efficiency (availability in Armenian and/or WCAG 2.1 compliance will be considered an advantage)		5
• Implementation roadmap, methodology, and risk management strategy		5
Infrastructure and Software Technology Support		20
• Compliance with ISO 27001 information security standards, disaster recovery mechanisms, and high availability (backup and recovery)		10
• Maximum compatibility with existing infrastructure/ecosystems		5
• Warranty and post-warranty support conditions		5
Supplier Experience and Industry Reputation		20



At least 3 years of experience in AML/CFT-related SupTech or financial regulatory ICT solutions, including successful implementation of AML/CFT regulatory projects across different jurisdictions (cross-border experience is preferred).		16
Partner Certifications and Client Reference Letters		4
Core Team Experience and Implementation Team Competencies		10
Collective Assessment of Personnel Qualifications		10
Training and Training Materials		10
Training Framework and Supporting Materials		10
System Presentation		10
Detailed and Comprehensive Presentation of the System Functionality		10
Total Technical Score		100

SPECIAL CONDITIONS

1. All components of the software must be provided under a subscription model for a period of at least 5 years from the date of installation.
2. There must be no publicly available information on the manufacturer's website indicating an end-of-support or end-of-life date for the offered software products.
3. Technical support must be available in 24x7 mode, with the ability to register support tickets (including, if necessary, through the manufacturer's system), record incidents (service cases), and receive a response within a maximum of 4 hours.
4. The System implementation date shall be considered the date on which the final acceptance certificate is signed. This date will also serve as the reference point for the calculation of maintenance and/or support service extensions, where applicable.
5. For price comparison purposes, the Client may also consider optional items (if required by this Technical Terms of Reference). The Client reserves the right to procure optional items during the contract period at the same quoted price, as needed.



CONTRACTUAL TERMS

1. The Contract shall enter into force upon signature by both Parties and shall remain valid until full performance of the obligations assumed by the Parties under the Contract. The final deadline for the complete fulfillment of these obligations is set at six (6) months from the date of contract signing, with the possibility of extension subject to mutual agreement between the Parties.
2. The System implementation shall be considered completed and accepted only upon the bilateral signing of the final acceptance certificates by the Client and the Contractor.
3. The acceptance of system implementation work shall be carried out according to a schedule that is mutually agreed upon and approved in advance, and shall follow the procedure outlined below:
 - 3.1. After the implementation of the system (or individual subsystems), the Client shall, within the timeframe defined in the mutually agreed and approved schedule, review the quality of the work performed and its compliance with the requirements specified in the Contract.
 - 3.2. If no deficiencies are identified, the Client shall sign the relevant acceptance certificate(s).
 - 3.3. In the event deficiencies are detected, the Contractor shall be obliged to remedy them at its own expense within ten (10) working days. Only upon successful correction of the deficiencies shall the relevant acceptance certificate be signed.
4. Payment shall be made within five (5) working days following the signing of the relevant acceptance certificate(s) by both Parties and the issuance of the corresponding tax invoice by the Contractor.
5. The provision of post-warranty maintenance services, procedures for acceptance and handover, and payments related to staff training after system implementation shall be defined in the Contract.
6. In the event the Contractor fails to meet the deadlines stipulated in the Contract, a penalty shall be imposed for each delayed working day of service provision. The penalty shall amount to 0.1% of the value of the outstanding (unperformed) services, subject to the legally established maximum annual limits.
7. In the event of delayed payments by the Client, a penalty of 0.1% of the unpaid amount shall accrue for each delayed business day, also subject to the maximum annual penalty limit as prescribed by applicable law.
8. The Client shall have the right to deduct, without acceptance, any penalties payable by the Contractor from the amounts due to the Contractor under the Contract.