



ANNOUNCEMENT regarding the organization of an open tender

*The text of this Announcement has been approved by the Tender Committee of the Central Bank of Armenia
Protocol No. 52 dated 18th of December, 2025.*

The Central Bank of Armenia announces a Tender, the terms of which are presented in the attached Invitation.

Issued on:	09.01.2026
Procuring entity:	Central Bank of Armenia 6 Vazgen Sargsyan St., Yerevan, 0010, Armenia
Procedure Reference Number:	CBA-2026-001
Purpose of Procedure:	<u>PROCUREMENT OF A SYSTEM FOR AUTOMATING ML/FT AND SANCTIONS COMPLIANCE RISK ASSESSMENT AND MONITORING PROCESSES, AND FOR THE PROVISION OF SYSTEM TECHNICAL SUPPORT AND MAINTENANCE SERVICES FOR THE SYSTEM FOR THE NEEDS OF THE CENTRAL BANK OF THE REPUBLIC OF ARMENIA</u>
Publication place:	https://www.cba.am/en/SitePages/tenders.aspx
Deadline for Submission of Proposals:	Thursday, the 19th of February, 2026, not later than 4:00 p.m. (GMT+4)
Submission method:	In electronic form, by sending an e-mail to the following address: CBA-2026-001@cba.am
Deadline for Requests for Clarifications of the Invitation:	Friday, the 13th of February, 2026, not later than 4:00 p.m. (GMT+4)
Date of Opening of Proposals:	Thursday, the 19th of February, 2026, 4:00 p.m. (GMT+4)
Notification of Award:	Thursday, the 05th of March, 2026, 4:00 p.m. (GMT+4)
Tender Organized By:	Central Bank of Armenia, Procurement Coordination Service
Communication method:	In written form only, to procurement@cba.am

The Bidder selected through this procedure will be awarded a contract for the supply and implementation of a system for automating ML/FT and sanctions compliance risk assessment and monitoring processes, as well as for the provision of system technical support and maintenance services for the needs of the Central Bank of the Republic of Armenia.



Central Bank of the Republic of Armenia

INVITATION TO AN OPEN TENDER

Request for Proposals

**FOR PROCUREMENT OF A SYSTEM FOR AUTOMATING ML/FT AND
SANCTIONS COMPLIANCE RISK ASSESSMENT AND MONITORING
PROCESSES, AND FOR THE PROVISION OF SYSTEM TECHNICAL SUPPORT
AND MAINTENANCE SERVICES FOR THE SYSTEM FOR THE NEEDS OF THE
CENTRAL BANK OF THE REPUBLIC OF ARMENIA**



TABLE OF CONTENTS

1.	DESCRIPTION OF SUBJECT OF PROCUREMENT.....	1
2.	BIDDER PARTICIPATION REQUIREMENTS AND QUALIFICATION CRITERIA.....	1
3.	PROPOSAL SUBMISSION PROCEDURE.....	4
4.	PRICE PROPOSAL.....	6
5.	CLARIFICATION OF INVITATION AND PROCEDURE FOR MAKING CHANGES TO THE INVITATION.....	8
6.	OPENING, EVALUATION OF PROPOSALS AND NOTIFICATION OF AWARD.....	9
7.	BID SECURITY	13
8.	CONTRACT EXECUTION AND/OR QUALIFICATION SECURITIES, ADVANCE PAYMENT SECURITY	15
9.	EXECUTION OF THE CONTRACT.....	17
10.	DECLARING THE PROCEDURE INVALID.....	17
11.	BIDDERS' APPEAL RIGHTS.....	18
	Appendix 1.....	19
	Appendix 2	156
	Appendix 2.1	159
	Appendix 3.....	164
	Appendix 3.1.....	167
	Appendix 3.2	169
	Appendix 4	170
	Appendix 5.....	171
	Appendix 6.....	172



This invitation is issued in addition to the Announcement of an Open tender (hereinafter also referred to as the “procedure”) conducted under reference number CBA-2026-001.

This invitation has been prepared in accordance with the legislation of the Republic of Armenia, the Law of the Republic of Armenia “On Procurement” (hereinafter referred to as the Law), and other applicable legal acts.

Within the scope of this procedure, payments for the technical maintenance and support services for the system over the subsequent five - year period, shall be made in accordance with the Article 15 part 6 of the Law of the Republic of Armenia “On Procurement”.

Payments for services in each subsequent fiscal year shall be conditional upon the allocation of the relevant financial resources.

If such financial allocations are confirmed, the contract remains in force. If they are not confirmed, the Procuring Entity shall notify the Supplier in advance, within the timeframes defined by the contract. In such cases, the Supplier shall not be obligated to provide services, and the Procuring Entity shall not be obligated to pay for them.

In the absence of allocated financial resources, the Procuring Entity reserves the right to unilaterally terminate the performance of the Contract.

All persons, including foreign individuals or organizations and stateless persons, are eligible to submit Proposals.

The Procuring Entity reserves the right to disregard in the contract any condition (or other information/data) in the proposal that is not expressly stipulated in this Invitation.

All matters related to this procedure shall be governed by the laws of the Republic of Armenia. Any disputes in relation to this procedure shall be examined and resolved by the courts of the Republic of Armenia.

The e-mail address of the Secretary of the Tender Committee is:
siran.yeganyan@cba.am.



1. DESCRIPTION OF SUBJECT OF PROCUREMENT

1.1. The subject of this procurement is the system for automating ML/FT and sanctions compliance risk assessment and monitoring processes, and the provision of system technical support and maintenance services (hereinafter also referred to as the “Product”) for the needs of the Central Bank of the Republic of Armenia (hereinafter also referred to as the “Bank” or the “Purchaser”).

1.2. Through this RFP, the Bank seeks to engage experienced and capable firms to provide a comprehensive software solution for the effective identification, assessment, and management of ML/FT and international sanctions compliance risks, including system deployment, configuration, training, and ongoing support and maintenance following implementation.

1.3. In accordance with this procedure, the purchase shall be carried out in a total of 1 (one) Lot.

1.4. The Terms of Reference, attached as per Appendix 1, form an inseparable part of this RFP and establish the minimum technical, functional, non-functional, and security requirements applicable to the solution. All requirements in the ToR must be fully addressed in the Bidder’s proposal. These requirements shall be included in and shall govern the execution of the Contract.

2. BIDDER PARTICIPATION REQUIREMENTS AND QUALIFICATION CRITERIA

2.1. The following persons may not be eligible to participate in this procedure:

- 1) persons who have been declared bankrupt by a court as of the date of submission of the proposal;
- 2) persons who, or whose executive body representative, have been convicted within the 5 (five) years preceding the date of submission of the proposal, of financing terrorism, crimes involving child exploitation or human trafficking, creating or participating in a criminal partnership, receiving, giving or brokering bribes, or crimes against economic activity as defined by law, except where the conviction has been removed or extinguished in accordance with the law;
- 3) persons in respect of whom an administrative act establishing liability for anti-competitive agreements, abuse of dominant position, or unfair competition in the field of procurement became final within the 3 (three) years preceding the date of submission of the proposal, or was upheld unchanged in the event of an appeal;



- 4) persons who, as of the date of submission of the proposal, are included in the list of bidders prohibited from participating in procurement processes, published in accordance with the procurement legislation of the member states of the Eurasian Economic Union. The condition does not apply to procurement processes financed under international agreements;
- 5) persons who, as of the date of submission of the proposal, are included in the list of bidders prohibited from participating in the procurement process;

If a bidder is included in a list referred to in sub-clauses 4 and 5 of this clause after the date of submission of the proposal, the proposal shall not be subject to rejection.

A bidder may be included in the aforementioned list if the bidder:

- violated a contractual obligation or an obligation assumed within the framework of a procurement process, resulting in unilateral termination of the contract by the Purchaser, termination of the bidder's right to further participation in the procurement process, or failure to pay the prepayment, contract performance security amount within the period specified in the invitation and/or contract;
- refused to execute a contract as a selected bidder or was deprived of the right to execute the contract.

2.2. To assess a bidder's eligibility to participate, together with the proposal, a written statement must be provided approved by the bidder in accordance with clause 2.1 of Part 2 of this invitation. No other documents or justifications may be required from the bidder, including from the selected bidder, for the assessment of eligibility. The authenticity of the bidder's statement shall be evaluated by the Tender Committee (hereinafter referred to as the "Committee") under the conditions set forth in this invitation.

2.3. Inclusion of a bidder in the list referred to in sub-clause 5 of clause 2.1 of Part 2 of this invitation automatically results in the restriction of the right of affiliated persons to participate in the procurement process for the duration of the bidder's inclusion in the list.

2.4. Simultaneous participation in this procedure of affiliated persons as defined in this clause, and/or organizations founded by the same person(s) or with more than 50 % (fifty percent) ownership by the same person(s), is prohibited, except in cases of participation by state or municipalities-founded organization and/or through a joint venture (JV) or consortium.



2.5. A bidder who declared the selected bidder shall provide a contract performance security in the manner and amount specified in this Invitation.

The Purchaser may waive the requirement to provide a contract performance security if, as of the date of Proposal opening, the selected bidder, or the organization providing services under this procedure as its officially authorized representative holds a credit rating equal to or higher than the sovereign credit rating of the Republic of Armenia, as assigned by a reputable international credit rating agency (such as Fitch Ratings, Moody's Investor Services, or S&P Global Ratings).

2.6. Bidders can participate in this procedure as joint ventures (consortium). In such cases:

- 1) the proposal shall include a joint venture agreement;
- 2) the joint venture shall nominate an Authorized representative who shall have the authority to conduct all business for and on behalf of any and all the members of the JV during the bidding process and, in the event the JV is awarded the Contract, during contract execution.
- 3) the Proposal shall be signed by an authorized representative of the JV on behalf of the JV, and so as to be legally binding on all the members as evidenced by a Power of Attorney signed by their legally authorized representatives.
- 4) during evaluation, the combined qualifications of all members to the joint venture shall be taken into account.
- 5) participants shall bear joint and several liability. If a consortium member withdraws, the contract concluded by the Purchaser with the consortium shall be unilaterally terminated, and the liability measures stipulated in the contract shall apply to the consortium members.
- 6) any party to the joint venture agreement may not submit a separate Proposal for the same procedure. Failure to comply with this requirement will result in the rejection of both joint venture Proposal and the separately submitted Proposal(s) at the Proposal opening session.

2.7. The bidder must demonstrate adequate experience, technical capability, and resources to fully perform the contractual obligations. The eligibility and qualification criteria are defined in Terms of Reference as per Appendix 1 to this Invitation. Only proposals that meet the following minimum qualification requirement shall be shortlisted for further evaluation:

2.7.1. The criterion of "**Professional experience**" will be evaluated as follows:



- At least 3 (tree) 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).

2.7.2. The criterion of "**Human resources**" will be evaluated as follows:

- Allocation of a qualified project team with a minimum of 5 (five) years of relevant professional experience, demonstrating proven involvement in the successful implementation of similar projects, and possessing expertise in AML/CFT compliance, regulatory reporting, software integration, and cybersecurity, ensuring timely and high-quality delivery of the Contract objectives.

3. PROPOSAL SUBMISSION PROCEDURE

3.1. To participate in this procedure, a bidder must submit a proposal to the Committee. A proposal is an offer submitted by the bidder based on this Invitation.

3.2. Bidders may not submit more than one proposal for the same procedure, except when submitting amendments to the proposal provided for in clauses 3.9 and 5.7 of this Invitation.

3.3. Proposals must be submitted to the Committee no later than the proposals submission deadline specified in the announcement of this procedure.

3.4. Proposals must be submitted electronically to CBA-2026-001@cba.am.

The documents must be submitted either in signed printed (scanned) format or in PDF format with electronic digital signatures.

3.5. Proposals for this procedure may be submitted in Armenian or English.

3.6. When submitting a proposal electronically, the following rules must be followed:

- The Reference Number "CBA-2026-001" must be included in the "Subject-line" of the e-mail.
- The proposal must be attached in **PDF format** only as one complete document, maintaining the order of documents specified in clause 3.10 of this Invitation.
- The attachments **must not** be submitted as a **Google Drive link**, **.rar file**, or in any similar link format.



- The total size of the email, including attachments, **must not exceed 25MB**. Bidders are responsible for ensuring that their electronic submissions comply with this limitation.
- If the files exceed the file size limit, the submission may be split into multiple emails, each clearly labeled (e.g., 'Part 1 of 3,' 'Part 2 of 3,' etc.).
- All attachments must be scanned for viruses prior to submission.
- The body of the email must contain plain text only and must not include any links.

Failures to comply with these rules may result in the Proposal being blocked by the Purchaser's virus protection system and not delivered. The Purchaser bears no responsibility in such cases.

Non-adherence may lead to the Proposal being deemed non-compliant and ineligible for evaluation.

It is strongly recommended that bidders submit their proposals at least 1-2 hours before the deadline to ensure timely delivery and to avoid potential technical issues.

An automatic reply e-mail will be sent to the bidder as confirmation of receipt of the proposal.

3.7. The Purchaser shall not be responsible for the receipt of emailed Proposals submitted after the deadline.

3.8. Proposals that do not comply with the requirements of Part 3 of this Invitation shall be rejected by the Committee at the Proposal opening session.

3.9. Bidders may amend or withdraw their Proposals before the Proposal submission deadline.

- In the event of an amendment, the revised Proposal must be sent to the email address specified in clause 3.4, following the procedure set out in this Part, with the subject line containing the phrase "Amendment to Proposal".
- To withdraw a Proposal, a notice of cancellation must be sent to procurement@cba.am.

3.10. **The bidder must submit the minimum set of following documents:**

- 1) **Application-statement** approved by the bidder in accordance with Appendix 2 attached to this Invitation, which includes:
 - a) a certification of compliance of the bidder and related persons with the participation requirements established by this Invitation,



- b) a statement confirming the absence of unfair competition, abuse of a dominant position, and anti-competitive agreements within the scope of this procedure,
 - c) a statement confirming the absence of separate participation in the procedure by any persons affiliated with the bidder and/or organizations founded by or with more than 50% (fifty percent) ownership by the bidder,
 - d) a declaration of actual beneficiaries, in accordance with Appendix 2.1 to this Invitation (not required if the bidder is an individual entrepreneur or natural person).
- 2) A document confirming the **bid security** for participation in the tender,
 - 3) The **financial proposal**, completed in accordance with Appendix 3 to this Invitation,
 - 4) **Breakdown of the financial proposal**, completed in accordance with Appendix 3.1 and 3.2, including proposed payment terms and conditions,
 - 5) **The technical proposal**, including the detailed description of the proposed solution, prepared in accordance with Appendix 4,
 - 6) **Company Portfolio**, completed in accordance with Appendix 5,
 - 7) **Organizational and Governance Overview**, completed in accordance with Appendix 6,
 - 8) Any other supporting documents and information specified in Terms of Reference of this Invitation, including those that demonstrate the bidder's capacity, experience, or other qualifications supporting its proposal.
 - 9) A **draft version of the contract** outlining the principal terms, conditions, responsibilities, and other relevant provisions (if available).

4. PRICE PROPOSAL

4.1. The proposed price, shall include, in addition to the cost of the Project, all expenses related to transportation, insurance, duties, taxes, and other charges, and may not be lower than their actual cost.

4.2. The bidder must submit the price proposal as a calculation consisting of the price (the sum of all costs) and the value-added tax ((VAT), applicable for resident bidders) for each Lot. If the bidder has to pay VAT to the state budget of the Republic of Armenia for the given transaction, the amount of VAT should be indicated separately.



4.3. The bidder must attach to the price proposal a detailed breakdown of the price of each component included in a given Lot.

4.4. The comparison of bidders' price proposals (Appendix 3) will be carried out excluding the amount of VAT mentioned in this clause.

The evaluation of the bidder's price proposal shall distinguish between material and non-material deviations. A proposal shall not be rejected on the basis of a non-material deviation. Non-material deviations include, but are not limited to, the following cases:

- a. the "Price" and "VAT" columns of the price proposal are completed using numbers only, while the "Total Price" column is completed using both words and numbers or only words;
- b. a discrepancy exists between the amounts stated in words or numerals in the "Price" and "VAT" columns, but the sum of any of the amounts indicated in either the words or numerals corresponds to the amount indicated in words in the "Total Price" column;
- c. the Lot number is indicated incorrectly in the price proposal but the name of the purchase item is correctly filled in;
- d. fractional monetary units in the "Price", "VAT", and "Total Price" columns are rounded down to the nearest whole number when below five-tenths and rounded up when at or above five-tenths;
- e. The "Price" and "VAT" columns contain matching amounts in words and numerals, while the "Total Price" column contains extra words resulting in a non-existent or incorrect number – in this case, the Committee will base its assessment on the sum of the amounts written in words in the "Price" and "VAT" columns.
- f. fractional monetary units of amounts written in words are indicated with numbers.

4.5. The proposal shall be rejected if it contains a material deviation, that alters or impacts the bidder's actual offered price, creates ambiguity in determining the price, or may influence the competitive ranking of bids.

4.6. The price proposal document as per Appendix 3 is not subject to correction.



4.7. The financial proposal for non-resident participants of the Republic of Armenia shall be expressed in United States Dollar or Euro. In such case, for Proposal evaluation and comparison purposes all prices expressed in foreign currency will be converted into Armenian Dram (AMD). The conversion shall be conducted by the Purchaser, with the exchange rate announced at its official website “www.cba.am” by the Purchaser on the date of opening of Proposals. Moreover, a contract will be executed in the same currency as submitted in the proposal.

4.8. In the event that the contract is concluded with a non-resident of the Republic of Armenia, profit tax shall apply, calculated at a rate of twenty percent (20%) of the contract price and shall be paid by the Purchaser. The applicable tax rate may be subject to change in the presence of a Double Taxation Avoidance Agreement between the countries of the Purchaser and the Bidder. In such cases, the selected Bidder must submit a Certificate of Tax Residency issued by the tax authority of their country within ten (10) calendar days from the date of signing the contract.

4.9. If the bidder is subject to profit tax, the comparison of price proposals shall be carried out based on the total value including the profit tax.

5. CLARIFICATION OF INVITATION AND PROCEDURE FOR MAKING CHANGES TO THE INVITATION

5.1. Bidders may request clarifications from the Committee in writing, no later than the deadline specified for Clarification Requests under this Invitation by sending a request to procurement@cba.am.

5.2. Clarifications shall be provided to bidders who have submitted a written request within 2 (two) working days following the date of receipt of the request.

5.3. On the day the clarification is provided, the content of the request and the clarification shall also be published on the official website “www.cba.am” under the “Tenders” section, without disclosing the identity of the bidder who submitted the request.

5.4. Clarification shall not be provided if the request was submitted after the deadline specified in this section, if the request falls outside the scope of the Invitation, or if responding to the request would involve the risk of disclosing state secrets.

5.5. Clarification shall not be provided if the inquiry concerns the correspondence between the technical specifications proposed by the bidder and those stipulated in this Invitation.

5.6. Changes to the Invitation can be made up to 5 (five) working days before the proposal submission deadline. Within 3 (three) working days of such changes, an announcement detailing



the modifications and their terms will be published on the official website “www.cba.am”, under the “Tenders” section. In the event of changes to the Invitation, the proposal submission deadline shall be adjusted and recalculated, as appropriate, based on the date of issuance of the change notice and the nature of the modification.

5.7. If changes are made to the Invitation, bidders have the right to amend their proposals in accordance with the procedure set forth in this Invitation. The Purchaser shall not be liable for any losses incurred by bidders as a result of changes to the terms of the Invitation.

6. OPENING, EVALUATION OF PROPOSALS AND NOTIFICATION OF AWARD

6.1. The Committee’s proposal opening session shall be convened at the Central Bank of the Republic of Armenia, 6 Vazgen Sargsyan St., Yerevan, on the date and time specified in the Announcement.

6.2. At the proposal opening session, the Committee shall evaluate:

- compliance with the procedure established by this Invitation for the electronic preparation and submission of proposals,
- the presence of the required documents in each proposal and their compliance with the requisites stipulated in the Invitation.

6.3. The Secretary of the Committee shall announce the price proposals of the bidders, expressed in a single number, based on the amount written in words.

6.4. The session for reviewing the results of the proposal evaluation shall be convened at the Central Bank of the Republic of Armenia, 6 Vazgen Sargsyan St., Yerevan, on the date and time specified in the Announcement.

6.5. The Committee may change the date and time of the notification of award by notifying the bidders.

6.6. Proposals shall be evaluated in accordance with this Invitation.

6.7. Proposals that meet the conditions set forth in this Invitation shall be deemed satisfactory; otherwise, they shall be deemed unsatisfactory and rejected. The Committee rejects proposals for which a price proposal is missing or presented inconsistently with the Invitation.

6.8. Proposals will be evaluated based on **non-financial** and **financial** criteria. The non-financial evaluation includes the bidder’s **qualification criteria** and the **technical proposal**, which together carry a total weight of **70%**. The **financial proposal** carries a weight of **30%**. The



contract shall be awarded to the bidder achieving the **highest combined total score** from both the non-financial and financial evaluations.

6.9. After the evaluation of the technical proposal and qualification criteria, candidates who have obtained a minimum of 70 points out of max 100 points will be considered for the financial proposal evaluation.

The table below shows the breakdown of technical and qualification criteria. The Total Technical Score assigned to each Proposal in the Evaluation will be determined by adding and weighting the scores assigned by the Tender Committee to technical features of the Proposal in accordance with the criteria set forth below.

Evaluation of technical and qualification criteria - Summary of Evaluation Focus	Weight (%)	Maximum Score
Technical Proposal Evaluation	70	
Functional and Methodological Suitability, and Degree of innovation		30
Alignment with the functional and technical requirements defined in this RFP 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 and a detailed implementation plan with a clear timeline, 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 technical support and maintenance service 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

6.10. In this methodology, the Financial Criteria weight is 30%. Accordingly, the maximum number of points assigned to the financial proposal is allocated to the lowest price proposal. All other price proposals receive points in inverse proportion. The formula is as follows:

$$P = y (p/z)$$

Where:

- P = points for the financial proposal being evaluated
- y = maximum number of points for the financial proposal
- p = NPV of the lowest priced proposal
- z = NPV of the proposal being evaluated.

During the price proposal comparison, not only the offered price is evaluated, but also the Net Present Value (NPV) of each proposal, taking into account all expected payments over the duration of the contract. The present value is calculated using the discount rate defined by the Procuring Entity.



Additionally, the evaluation and comparison of the price proposals shall be conducted excluding the amount of tax (VAT) specified in Article 4.2 of this Invitation.

6.11. The Committee shall determine and announce which bidders have been selected and which have not, from among those whose proposals were deemed to meet the requirements of the Invitation. In the event of equal combined scores:

- a. simultaneous negotiations shall be conducted with the concerned bidders to achieve a price reduction and determine the selected bidder,
- b. the Secretary of the Committee shall simultaneously and electronically notify the concerned bidders of the terms, duration, day, time, and place of the negotiations,
- c. based on the prices offered during the negotiations, the selected and non-selected bidders shall be determined and announced. If the combined scores remain equal after negotiations, the preference shall be given to the proposal with lower price.

6.12. If the prices proposed by bidders meeting the requirements of the Invitation exceed the estimated/budgeted cost, the Committee may either declare the procurement procedure invalid or declare the bidder who submitted the lowest price proposal the selected bidder, provided that the rights and obligations of the parties under the contract come into effect only if additional financial resources are allocated and an agreement on that basis.

6.13. If the evaluation of a proposal reveals inconsistencies with the requirements of the Invitation, the Secretary of the Committee shall notify the bidder electronically and offer the opportunity to correct the discrepancy.

6.14. If the bidder corrects the discrepancy within upon agreed time, the proposal shall be considered satisfactory. Otherwise, the proposal shall be deemed insufficient and rejected.

6.15. A Committee member or Secretary shall not participate in the Committee's work if it is revealed that an organization founded by that member or Secretary, or in which they have a share, or a person related to them by close kinship or in-law relationship (parent, spouse, child, sibling, grandparent, or grandchild, as well as spouse's parent, child, sibling, grandparent, or grandchild) or an organization founded or owned by that person, has submitted a proposal. In such as case, the Committee member or Secretary shall immediately withdraw from the procedure.

6.16. After the proposals are opened and finalized, a protocol shall be drawn up according to the established procedure and signed by the Committee present at the session.



6.17. Bidders may request copies of the Committee meeting minutes, which will be provided within 1 (one) working day. Bidders or their representatives may attend the proposal opening and award notification sessions by emailing the Procurement Coordination Service at procurement@cba.am at least 1 (one) day in advance, including their name, surname, and organization. Bidders must present an identity document, and representatives must provide a valid power of attorney. Copies of the commission's meeting minutes can be requested and will be provided within one working day.

6.18. The proposals shall be evaluated, and selected bidder determined, per individual Lot.

6.19. If the selected bidder refuses to sign the contract or becomes ineligible to execute it, the next ranked bidder shall be recognized as the selected bidder by decision of the Committee.

6.20. The Committee may verify the authenticity of the information submitted by the bidder through official sources or by obtaining a written opinion from the relevant authorities. In such cases, the relevant state and local self-government bodies shall provide a written conclusion within 2 (two) working days following the receipt of the request. If the submitted information is found to be untrue, the bidder's proposal shall be rejected.

6.21. Before contract execution, the Purchaser shall notify all bidders of the decision regarding contract award no later than the 1 (one) working day following the adoption of the decision on the selected bidder. The decision shall include summary information on the evaluation of proposals, the justification for selecting the winning bidder, and a statement on the inactivity period.

7. BID SECURITY

7.1. The Bidder shall, together with the Proposal, provide a bid security. The amount of the bid security shall be 2 (two) percent of the price proposed in the Proposal for the implementation costs.

7.2. The bid security shall be provided in the form of:

- Cash or;
- a bank guarantee, valid for at least 90 working days starting from the Deadline for Submission of Proposals.

The bid security provided in cash shall be transferred to the Purchaser's account No. 103001702119 (indicating the purpose: "Bid Security – [procedure code]").

For AMD: N 103001702119



For USD: Beneficiary's Bank: JPMorgan Chase Bank, NY
SWIFT code: CHASUS33
Beneficiary: Acc. No:001-1-010782
Central Bank of the Republic of Armenia
SWIFT (BIC) code: CBRAAM22

For EUR: Beneficiary's Bank: Commerzbank, Frankfurt, Germany
SWIFT BIC: COBADEFF
Beneficiary: Acc. No: 400886424101
Central Bank of the Republic of Armenia
SWIFT (BIC) code: CBRA AM 22

7.3. The bid security, in the form of a bank guarantee, should be provided by the Issuing Bank through an authenticated SWIFT message not later than upon agreed deadline to the Advising Bank. The Guarantee should be submitted in paper form upon request. In addition, a scanned copy of the original guarantee may also be provided.

7.4. The bid security shall be returned within 5 (five) working days after the contract is signed. If the procurement procedure is declared unsuccessful, the bid security shall be returned within 5 (five) working days after the expiration of the inactivity period.

In the case of a Bank guarantee, the Purchaser shall release the guarantee through an authenticated SWIFT message within the timeframes specified in this clause regarding the return of the bid security.

7.5. The bidder shall pay the bid security (i.e. it shall not be returned) if the bidder:

- 1) is selected as the winning bidder but refuses or is deprived of the right to execute the contract;
- 2) violates an obligation undertaken within the framework of the procurement process, resulting in the termination of the bidder's further participation in the process.

In case of Bank Guarantee, the Purchaser shall submit the demand for payment to the Issuing Bank by authenticated SWIFT message within 5 (five) working days following the date on which the basis for the payment of the guarantee arises, but not later than the maturity date of the guarantee.

7.6. Banks use third correspondent banks for sending an authenticated SWIFT message if they haven't RMA Exchange with each other in place. All associated costs related to the issuance,



transmission, and confirmation of the guarantee, including any intermediary bank fees, shall be borne by the bidder.

8. CONTRACT PERFORMANCE AND ADVANCE PAYMENT SECURITIES

8.1 Based on the requirement to provide contract performance security, within 20 (twenty) working days from the date of receipt of the relevant notification in the case of bank guarantee and 5 (five) working days in the form of cash, the selected bidder shall provide contract performance security.

8.2 The amount of contract performance security shall be 10 (ten) percent of the implementation costs for the implementation period. The final terms of the security shall be discussed and agreed with the selected bidder. The contract performance security shall be provided in the form of cash or a bank guarantee. The guarantee must be valid at least until the 90th working day following the date of the final acceptance act.

- In the case of a bank guarantee, the contract security shall be submitted in a format approved by the Purchaser prior to contract signature. The contract security, in the form of a bank guarantee, should be provided by the Issuing Bank through an authenticated SWIFT message not later than upon agreed deadline to the Purchaser. The Guarantee should be submitted in paper form upon request. In addition, a scanned copy of the original guarantee may also be provided. Banks use third correspondent banks for sending an authenticated SWIFT message if they haven't RMA Exchange with each other in place. All associated costs related to the issuance, transmission, and confirmation of the guarantee, including any intermediary bank fees, shall be borne by the bidder.
- Contract performance security provided in cash shall be transferred to the Central Bank's bank account (the procedure reference number must be indicated in the "Purpose" field):

For AMD: N 103001702119

For USD: Beneficiary's Bank: JPMorgan Chase Bank, NY

SWIFT code: CHASUS33

Beneficiary: Acc. No:001-1-010782

Central Bank of the Republic of Armenia

SWIFT (BIC) code: CBRAAM22



For EUR: Beneficiary's Bank: Commerzbank, Frankfurt, Germany

SWIFT BIC: COBADEFF

Beneficiary: Acc. No: 400886424101

Central Bank of the Republic of Armenia

SWIFT (BIC) code: CBRA AM 22

8.3 A contract shall be signed with the selected bidder if the latter provides the required contract performance security.

8.4 If a contract executed within the framework of a multi-component (lot) procurement procedure is terminated due to non-performance or improper performance of any individual component(s), the contract performance security shall be paid only in the amount calculated for the relevant component(s).

8.5 In case of Bank Guarantee, the Purchaser shall submit the demand for payment to the Issuing Bank by authenticated SWIFT message within 5 (five) working days following the date on which the basis for the payment of the guarantee arises, but no later than the maturity date of the guarantee. If the bank rejects the request due to incomplete documentation, the Purchaser shall submit a new request within 2 (two) working days of receiving the rejection.

8.6 The Purchaser shall return the contract performance security as follows:

- In the case of a Bank guarantee, the Purchaser shall release the guarantee through an authenticated SWIFT message within 5 (five) working days following the date on which the basis for return arises,
- In the case of a penalty, the Purchaser shall make a written notification regarding the return of contract performance security to the bidder who provided it, within 5 (five) working days following the date on which the basis for return arises.

8.7 If the contract provides for an advance payment by the Purchaser, the selected bidder shall also provide the Purchaser with advance payment security in the amount of the advance payment, in the form of a bank guarantee, valid at least until the 90th working day following the date of the final acceptance act.

8.8 The Purchaser shall notify the issuing bank in writing regarding the release of the advance payment security within 5 (five) working days following the date of the final acceptance act

8.9 The procedure for repayment of the advance payment is defined by the contract.



8.10 All bank guarantees shall be unconditional and irrevocable issued by a bank agreed with the Purchaser.

9. EXECUTION OF THE CONTRACT

9.1. The contract shall be executed by the Purchaser based on the decision of the Committee.

9.2. The period of inactivity for this procedure shall be 10 (ten) calendar days. The period shall not apply if only one bidder submits a proposal and a contract is executed with that bidder.

9.3. On the fourth working day following the expiration of the period of inactivity defined in clause 9.2 of this Invitation, the Purchaser shall electronically notify the selected bidder by submitting a proposal to execute a contract and the draft contract, which shall include a complete description of the product and services as set forth in the selected bidder's proposal. The contract may not be executed earlier than the fourth working day following the expiration of the inactivity period specified in clause 9.2 of this Invitation.

9.4. If, after receiving the notice of award and draft contract, the selected bidder does not approve the contract and submit the contract performance security to the Purchaser within the period stipulated in clauses 8.1 and 8.2 of this Invitation, the bidder shall be deprived of the right to sign the contract. The draft contract approved by the selected bidder shall be submitted to the Purchaser in writing.

9.5. Before the expiration of the period provided for in clause 9.4 of this Invitation, the parties may agree to make changes to the draft contract. Such changes shall not involve any material modifications to the description of the subject of the procurement, nor shall they result in an increase in the advance payment or the price proposed by the selected bidder.

9.6. The Purchaser shall execute the contract if no bidder appeals the decision to execute the contract within the inactivity period defined in this clause. The contract shall be deemed invalid if executed before the expiration of the inactivity period, without properly executing the contract, or following a notice declaring the procurement procedure to be invalid.

10. DECLARING THE PROCEDURE INVALID

10.1. The Committee shall declare the procedure to be invalid if:

- no proposals are submitted,
- none of the proposals meets the requirements of the Invitation,



- the procurement needs cease to exist,
- no contract is executed.

10.2. The Purchaser shall notify all bidders participating in the tender about the reason for declaring the procurement procedure invalid.

11. BIDDERS' APPEAL RIGHTS

11.1. All interested persons have the right to appeal the actions (or inactions) and decisions of the Purchaser and the Committee, in accordance with the procedure established by the Civil Procedure Code of the Republic of Armenia (hereinafter referred to as the “Code”).

11.2. All persons have the right to appeal the descriptions of the subject of procurement or the requirements of the Invitation before the deadline for submission of proposals, in accordance with the procedure established by the Code.

11.3. Relations related to this procedure are not administrative relations and are governed by the laws of the Republic of Armenia regulating civil law relations.



TEARMS OF REFERENCE

LOT	Name	Technical Description	Price (AMD)
1.	Procurement of system for automating ML/FT and sanctions compliance risk assessment and monitoring processes, and for the provision of system technical support and maintenance services for the system	The technical specification is presented in detail in Terms of Reference stated below	249,304,935 For the implementation period



1. 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).

2. 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 dynamic monitoring capabilities for FIs 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.

3. PLACE OF IMPLEMENTATION

The place of supply and implementation of the system is the Central Bank of the Republic of Armenia, located at 6 Vazgen Sargsyan Street, Yerevan, 0010, Republic of Armenia.



4. IMPLEMENTATION LOCATION

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

5. 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 support comprehensive data collection and integration to enable AML/CFT and sanctions compliance risk assessments. Specifically:

- **Survey Portal (Primary Source):** The System must provide an automated and secure survey portal as the primary mechanism for data collection, with built-in validation features to minimize errors. The portal shall also allow financial



institutions to upload supporting documents (e.g., AML policies, board approvals) as attachments to their survey responses, ensuring completeness of submissions.

- **Standardized File Ingestion:** In addition to survey data, the System must be capable of ingesting data from MS Excel or JSON standardized file formats.
- **API Integration:** The System shall support integration with external databases and systems via secure APIs, enabling direct ingestion of supervisory data.
- **ETL (Extract, Transform, Load):** The System shall support ETL processes to map, transform, and normalize data from APIs, files, and permissible databases, including scheduling, validation, and error reporting. Ingested data must be persisted and directly linked to risk models, ensuring that risk assessments are updated automatically. The vendor shall explicitly specify which ETL functions are provided as COTS configuration and which are professional services.

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. The System shall enable financial institutions to upload supporting documents to their survey answers, ensuring that all responses can be substantiated with appropriate documentation.

Support for MS Excel or Other Standardized Files: The System must accept information from MS Excel or JSON 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/minimizing 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/minimizing 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 email or SMS). 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) level and sector-wide level. The final output is a residual risk heatmap, providing supervisors with a comparative overview across FIs and sectors enabling risk-based prioritization of supervisory actions—specifically targeting high-risk institutions, high-risk sectors and critical risk 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, enabling supervisors to generate analytical and management reports across multiple dimensions, including risk factors, institutions, and sectors, and at varying frequencies (e.g., daily, monthly, or quarterly). While the AML/CFT risk estimation cycle is formally conducted on a quarterly basis, the System must also be capable of updating inherent risk estimates with a higher frequency, incorporating significant market developments and newly available data.

When such developments significantly affect inherent risk scores—and, by extension, residual risk estimates—the System must actively alert supervisors. Significance may be defined by thresholds, percentage changes, or other methods configurable by the supervisory authority. Alerts should be visible within the dashboard and optionally delivered through other channels (e.g., in-system notifications), ensuring supervisors can respond promptly. These alerts must allow supervisors to re-evaluate risk scores, adjust supervisory priorities, and update action plans in a timely manner.

Users must be able to define parameters and apply filters—such as time periods, sectors, or jurisdictions—to tailor reports to their needs. The System must generate both visual outputs (e.g., charts and dashboards) and tabular reports that present data values over



time. It must support both scheduled and on-demand report generation and provide pre-designed templates, while also allowing users to create, customize, and save templates for regular use. Reports must be exportable in widely used formats (e.g. MS Excel, PDF).

To ensure accuracy, the System must validate incoming data and automatically refresh reports whenever new data is imported. Role-based access control must govern who can create, edit, or view reports, maintaining both security and compliance. Collectively, these features will provide supervisors with the tools to generate accurate, timely, and targeted reports while enabling proactive, risk-based supervisory action.

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.



6. DESCRIPTION OF FUNCTIONAL REQUIREMENT

No.	Requirement	ID	Description	Requirement Type	Delivery approach	Examples
1	<i>Surveys and Data Management</i>	-	-	-	-	-
1.1	Ability to Easily Create and Customize Specialized Surveys	R-01	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.	Mandatory Requirement		
		R-02	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.	Mandatory Requirement		
		R-03	Surveys should include conditional logic, branching options, and multilingual support, making them flexible for different situations.	Mandatory Requirement		



		R-04	<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.	Mandatory Requirement		
		R-05	<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.	Mandatory Requirement		
		R-06	<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	Mandatory Requirement		



			complexity to ensure logical sequencing.			
		R-07	<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.	Mandatory Requirement		
1.2	Ability to Easily Distribute and Collect Surveys, and Automatically Aggregate the Results	R-08	Surveys should be delivered and collected through the web portal as the primary channel. Financial institutions will access and complete questionnaires securely online, with invitations and reminders sent via email notifications only.	Mandatory Requirement		
		R-09	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.	Mandatory Requirement		



		R-10	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.	Mandatory Requirement		
		R-11	It should be possible to use aggregated data to generate custom reports and dashboards, offering a clear visual representation of survey outcomes.	Mandatory Requirement		
		R-12	The System should ensure secure storage of collected data by enforcing access controls to protect the integrity and confidentiality of survey responses.	Mandatory Requirement		
1.3	Survey Field Properties	R-13	Question Text: This should be the primary text displayed to the respondent.	Mandatory Requirement		



		R-14	Additional Description or Help Text: 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.”	Mandatory Requirement		
		R-15	Rich Text Editor: 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.	Mandatory Requirement		
		R-16	Links to Resources: 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.	Mandatory Requirement		



1.4	Types of Data Collected from Responses	R-17	Number: Allows the collection of simple numeric values (e.g., quantities, scores).	Mandatory Requirement		
		R-18	Currency: Supports the entry of monetary values, formatted as currency.	Mandatory Requirement		
		R-19	Percentage: Used to collect percentage values.	Mandatory Requirement		
		R-20	Segmented Numeric Data: Numeric entries categorized by jurisdiction, region, or any custom segmentation (e.g., sales by country, income by department).	Mandatory Requirement		
		R-21	Calculated Field: Represents a relationship between two numeric values. Automatically computes and displays the ratio or result between them.	Mandatory Requirement		
		R-22	Sum of Other Fields: Automatically calculates the total of selected numeric fields.	Mandatory Requirement		



	R-23	Binary: Captures yes/no or true/false type responses.	Mandatory Requirement		
	R-24	Single Choice: Allows respondents to select one option from a list (e.g., radio buttons for single selection).	Mandatory Requirement		
	R-25	Multiple Choice: Allows respondents to select more options from a list (e.g., checkboxes for multiple selections).	Desirable Requirement		
	R-26	Date: Collects specific dates in a standard format (e.g., DD/MM/YYYY).	Mandatory Requirement		
	R-27	Free Text: An open text field that allows respondents to enter unstructured textual responses.	Mandatory Requirement		
	R-28	Country Selector: A dropdown menu that allows respondents to select a country from a predefined list.	Mandatory Requirement		
	R-29	Custom Dropdown: A configurable dropdown list for selecting from predefined options, such as industry sectors, product types, or custom categories.	Mandatory Requirement		



		R-30	File Upload: Allows respondents to upload files or documents as part of their response (e.g., PDFs, Word documents).	Mandatory Requirement		
1.5	Survey Completion Features Based on Conditional Question Logic	R-31	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.	Mandatory Requirement		
		R-32	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.	Mandatory Requirement		
		R-33	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.	Mandatory Requirement		



		R-34	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.	Mandatory Requirement		
		R-35	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.	Mandatory Requirement		
		R-36	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.	Mandatory Requirement		



		R-37	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.	Mandatory Requirement		
		R-38	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.	Mandatory Requirement		
1.6	Validation of Survey Data Quality and Completeness	R-39	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.	Mandatory Requirement		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.
		R-40	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 within the 0–100 range). This ensures that each data point meets specific quality standards.	Mandatory Requirement		
		R-41	The System should also support customizable data validation rules that involve relationships between two or more data fields.	Mandatory Requirement		
1.7	Antivirus Scanning	R-42	Automatic Scanning on File Upload: When a file is uploaded, the System should automatically scan it for known viruses, malware, and other security	Mandatory Requirement		



			threats using integrated antivirus software.			
		R-43	Execution-Based Scanning: The antivirus scan should be triggered upon execution of the file upload process.	Mandatory Requirement		
		R-44	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.	Mandatory Requirement		
		R-45	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.	Mandatory Requirement		
1.8	Survey Rejection and Feedback	R-46	Rejection of Invalid Submissions: The System should allow supervisors to reject submitted surveys that do not meet predefined requirements or	Mandatory Requirement		



			contain errors. This ensures that only accurate, valid, and complete data is processed.			
		R-47	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).	Mandatory Requirement		
1.9	Survey Resubmission and Correction Workflow	R-48	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.	Mandatory Requirement		



		R-49	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.	Mandatory Requirement		
		R-50	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.	Desirable Requirement		
		R-51	Resubmission Without Restarting: After making the necessary corrections, users should be able to resubmit the survey without having to restart from scratch.	Mandatory Requirement		



1.10	Multi-Phase Survey Functionality	R-52	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.	Mandatory Requirement		
		R-53	Carry-Forward of Previous Responses: The System should allow responses from earlier phases to be carried over into subsequent survey phases.	Desirable Requirement		
		R-54	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.	Mandatory Requirement		



		R-55	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 (reporting cycles).	Mandatory Requirement		
		R-56	Cross-cycle Analytical Capabilities: The System must support comprehensive analysis across multiple supervisory cycles, enabling supervisors to identify trends, patterns, and changes over time. It should include visualization and comparison tools that allow users to track shifts in responses, highlight variations in risk assessments, and detect emerging risks early.	Mandatory Requirement		
1.11	Organizational List Management and Synchronization	R-57	Editable Organization Records: The System should allow supervisors to easily update the list of organizations when changes occur in organizational	Mandatory Requirement		



			data (e.g., name, contact information, or status).			
		R-58	Add, Update, or Remove Organizations: Users should be able to add new organizations, update the information of existing ones, or remove outdated entities.	Mandatory Requirement		
		R-59	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.	Mandatory Requirement		



		R-60	Synchronization with Distributed Surveys: All changes made to an organization's data should be automatically synchronized with previously distributed surveys.	Mandatory Requirement		
1.12	Notification and Messaging Features	R-61	<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.	Mandatory Requirement		
		R-62	<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.	Mandatory Requirement		
		R-63	<i>Deadline Extensions:</i> Notifications that inform participants about an extension of the deadline for completing or submitting a form.	Mandatory Requirement		



		R-64	<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.	Mandatory Requirement		
		R-65	<i>Submission Confirmation:</i> Users should receive confirmation notifications once a task, survey, or form is successfully submitted.	Mandatory Requirement		
		R-66	<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.	Mandatory Requirement		
1.13	Email Branding and Customization	R-67	<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.	Mandatory Requirement		



		R-68	<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.	Mandatory Requirement		
		R-69	<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.	Mandatory Requirement		
1.14	Survey Engagement Status Notifications by Institution	R-70	Inactive Financial Institutions (FIs): The email should indicate which financial institutions have not yet started the survey or have remained inactive since receiving the invitation.	Mandatory Requirement		
		R-71	Active (In-Progress) Financial Institutions: The System should distinguish those FIs currently working on the survey but who have not yet submitted their responses.	Mandatory Requirement		



		R-72	Submitted Financial Institutions: 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.	Mandatory Requirement		
1.15	Supervisor Access to In-Progress Surveys	R-73	Progress Monitoring of Partially Completed Surveys: 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.	Desirable Requirement		
		R-74	Real-Time Guidance and Feedback: Supervisors should have access to view in-progress responses and provide respondents with real-time feedback or guidance.	Mandatory Requirement		



		R-75	Deadline Tracking and Reminders: 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.	Mandatory Requirement		
1.16	Use of MS Excel files or other standardized file formats for ML/FT Inquiries	R-76	<i>File Acceptance:</i> In addition to the web portal as the primary source of data collection, the System must be able to accept MS Excel files or JSON files for the purpose of assessing ML/FT risks and the quality of their management. All such files must follow pre-defined templates to ensure consistency, accuracy, and comparability across all submissions.	Mandatory Requirement		.The template should include the required fields, such as the volume of cash transactions, the number of suspicious transactions, the number of resident and non-resident clients, and



						other relevant data.
		R-77	<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).	Mandatory Requirement		



		R-78	<i>Validation Rules:</i> Validation rules should include checks for missing data and incorrect formats. The System must enforce data integrity before further processing.	Mandatory Requirement		
		R-79	<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.	Mandatory Requirement		
		R-80	<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.	Mandatory Requirement		



	R-81	<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.	Mandatory Requirement		
	R-82	<i>Error Handling and Messaging:</i> If errors are detected in the submitted MS Excel or .JSON (e.g., missing fields, formatting issues), the System should notify the user with clear error messages indicating what needs correction.	Mandatory Requirement		
	R-83	<i>File Resubmission Workflow:</i> The System should provide a resubmission process that allows users to upload corrected files after validation failures.	Mandatory Requirement		
	R-84	<i>Template Version Control and Data Update Support:</i> The System should implement version control to manage updates to MS Excel or .JSON file templates. When configurations change, updated templates must	Mandatory Requirement		



			reflect the latest format and data requirements.			
1.17	API Integration	R-85	API Connectivity Support: The System should support integration with external systems via API for both data ingestion and data sharing.	Mandatory Requirement		
		R-86	Secure Authentication for API Connections: 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).	Mandatory Requirement		
		R-87	Error Handling and Retry Mechanisms: The System should include error handling capabilities and automated retry mechanisms for failed API	Mandatory Requirement		



			requests to ensure data consistency and reliability.			
		R-88	Data Mapping from API Inputs: Upon receiving data via API, the System should map external data structures to its internal data model to ensure proper storage and use.	Mandatory Requirement		
		R-89	Automated API Queries: The System should support automated execution of API requests enabling timely and efficient data exchange.	Mandatory Requirement		
		R-90	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.	Mandatory Requirement		
1.18	Automatic ETL Performance from Various Databases and	R-91	<i>Extract (Data Download)</i> : The System should automatically extract collected survey data according to predefined rules and formats,	Mandatory Requirement		



	Import of Query Results into Risk Models		ensuring consistency, accuracy, and readiness for further processing and analysis. Transform (Data Preparation): 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.			
		R-92	Load (Integration with Risk Models): 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.	Mandatory Requirement		
2.	<i>Risk Modeling</i>	-	-	-	-	-



2.1	Risk Assessment (Inherent Risk, Controls, and Residual Risk)	R-93	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.	Mandatory Requirement		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.
		R-94	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	Mandatory Requirement		For example, if a financial institution has an effective transaction monitoring System and strong KYC



			diligence (KYC) processes. The System shall generate a control quality score indicating the effectiveness of these controls in reducing inherent risk.			procedures, the System should assign a high control quality score—indicating that risks are being well-managed.
		R-95	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.	Mandatory Requirement		For example, if a high inherent risk is identified—due to large transaction volumes in a high-risk jurisdiction—but effective controls are in place, the residual risk may be
		R-96	In line with CBA’s methodology, residual risk is the combination of inherent risk levels and control/management quality scores within a heatmap framework. The System must therefore support configurable heatmap models that reflect supervisory methodology,	Mandatory Requirement		



			enabling supervisors to visualize how different levels of inherent risk and control effectiveness interact to produce the final residual risk outcome.			significantly reduced.
2.2	Risk Weighting and Aggregation	R-97	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.	Mandatory Requirement		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.
		R-98	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.	Mandatory Requirement		
2.3	Custom Hierarchical and Segmented Risk Assessment	R-99	<i>Defining Custom Hierarchies:</i> The System should allow users to define custom risk hierarchies based on the risk levels of clients or services.	Mandatory Requirement		For example, users can define high-risk clients based on their



			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).	Mandatory Requirement		presence in high-risk jurisdictions or involvement in specific economic sectors (e.g., the gambling industry).
			These classifications should be configurable, enabling supervisors to adjust the hierarchy based on emerging threats or changes in regulatory requirements.	Mandatory Requirement		For example, the System can group transactions based on client type and jurisdiction, enabling segmented risk assessments for high-risk clients engaged in
		R-100	<i>Segmented Risk Assessments.</i> The System should support segmented risk assessments for each defined group, based on customizable risk categories.	Mandatory Requirement		



						cross-border transactions.
			Each segment (e.g., high-risk clients, high-risk products/services) should be evaluated separately, and risk scores should be calculated based on weighted factors relevant to each risk dimension.	Mandatory Requirement		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.
			The System should allow flexible configuration of these weights and scoring rules, so that supervisors can adjust them as new risks or regulations emerge.	Mandatory Requirement		
2.4	Export Functionality for Risk Assessments	R-101	Export Formats: The System should allow users to export inherent risk and control quality assessment results in standard formats (e.g., MS Excel, PDF).	Mandatory Requirement		For example, the System should allow for the export of survey results, risk



		R-102	Detailed Content: Exported files should include detailed descriptions, calculations, and all relevant model parameters, ensuring traceability and transparency.	Mandatory Requirement		assessments, and risk classifications for each financial institution (FI).
		R-103	Structured Output: The exported files should be clearly structured to support easy documentation, review, and archiving by supervisory staff.	Mandatory Requirement		
		R-104	Audit Logging: All export actions should be logged, and export history shall be accessible to System administrators for monitoring and audit purposes.	Mandatory Requirement		
2.5	Regional Risk Models Built on the Risk Profiles of Individual Jurisdictions or Predefined Jurisdiction Lists, with the Ability to Assign	R-105	<i>Individual Jurisdiction Risk Factors:</i> Each country or jurisdiction should be assessed based on at least the following indicators:	Mandatory Requirement		For example, high-risk jurisdictions (e.g., countries known for financial secrecy
			Regulatory and legal frameworks	Mandatory Requirement		



	Different Risk Weights to Each Jurisdiction or List		Effectiveness of ML/FT controls	Mandatory Requirement		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.
			Inclusion on international sanctions or watch lists (e.g., FATF high-risk jurisdictions)	Mandatory Requirement		
			Political stability, level of corruption, and economic transparency	Mandatory Requirement		
		R-106	<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.	Mandatory Requirement		
		R-107	<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.	Mandatory Requirement		Lower-risk jurisdictions may be assigned lower weights.
		R-108	<i>Weighted Jurisdiction Scoring:</i> Each jurisdiction or list may be assigned different weights according to its risk	Mandatory Requirement		



			profile, influencing overall risk calculations in the System.			
2.6	Specific Regions (e.g., States or Provinces within a Jurisdiction) with Differentiated Risk Weights	R-109	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.	Mandatory Requirement		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	R-110	Custom List Creation: Users should be able to create and define custom lists based on organizational needs (e.g., currencies, assets, transaction types).	Mandatory Requirement		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.
		R-111	Support for High-Risk Categories: These lists may include high-risk currencies, sensitive products, or vulnerable customer groups.	Mandatory Requirement		
		R-112	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.	Mandatory Requirement		
2.8	Segmentation of Data Points by Country, Region, or Specific Lists	R-113	The System must allow users to segment transaction-related data by country, displaying the results based on the selected jurisdiction.	Mandatory Requirement		
		R-114	The System must support regional filtering and analysis by enabling the	Mandatory Requirement		



			analysis of data specific to designated geographical areas.			
2.9	Performance of Risk Assessments (Relative Risk) of Institutions Within the Given Sectors	R-115	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.	Mandatory Requirement		
		R-116	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.	Mandatory Requirement		
		R-117	The System must identify outliers through comparison based on ML/FT	Mandatory Requirement		



2.10			risk factors, revealing institutions with relatively higher or lower risk levels.			
	Ability to Transition from FI-Level Risk Assessments to Sectoral and National Risk Assessments (Absolute Risk)	R-118	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.	Mandatory Requirement		
		R-119	The System must automatically process data obtained from financial	Mandatory Requirement		



2.11			institutions' risk assessments as key input for sectoral and national risk assessments.			
		R-120	This processing should ensure that sectoral trends and risks identified at the FI level are directly fed into higher-level assessments.	Mandatory Requirement		
		R-121	These assessments should provide data that can serve as input for the National Risk Assessment (NRA).	Mandatory Requirement		
		R-122	These assessments should support the formulation of policy decisions, resource allocation, and regulatory strategies aimed at mitigating the identified risks.	Mandatory Requirement		
	Ability to Enable/Disable Data Points for Inherent Risk and Internal Control Assessment.	R-123	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	Mandatory Requirement		For example, the supervisor should be able to assess the customer's inherent risk and determine



			assessment (e.g., transaction volume, jurisdictional risk) and which should not. The same applies to the control/management quality assessment, where only active control criteria should affect the final score.			that transaction volume is no longer relevant for the assessment based on new regulations, and therefore disable that data point.
		R-124	Disabled data points should not contribute to the overall risk or control assessment, but they must remain accessible for potential future activation.	Mandatory Requirement		
		R-125	Only authorized users (e.g., designated supervisors or administrators) should have access to enable or disable these data points.	Mandatory Requirement		
		R-126	The System must enforce role-based access control to ensure that only	Mandatory Requirement		



			specific users can change the status of data points.			
		R-127	All changes to the enabled/disabled status of data points must be logged by the System.	Mandatory Requirement		
		R-128	The log should include who made the change and when it was made.	Mandatory Requirement		
		R-129	When a data point is enabled or disabled, the System must be able to recalculate inherent risk and control/management quality scores upon user instruction, ensuring that updated configurations are reflected in the results only when the user initiates the recalculation. In addition, the System must provide an option for users to make multiple configuration changes within a single session and then trigger recalculation on demand through a dedicated action (e.g., a “Recalculate” button).	Mandatory Requirement		



		R-130	System should provide configurable alerts, such as outliers and when exceeding a % change cycle on cycle.	Mandatory Requirement		
		R-131	The System should provide alerts or confirmation messages for critical changes that significantly affect risk or control assessment outcomes. Alerts must be triggered for actions such as deactivating the survey mode, rejecting an entity's survey, or updating country/jurisdiction lists. For configuration changes such as enabling/disabling data points, adjusting thresholds, or modifying weightings, the System should not issue alerts by default but must log these changes in the audit trail and provide recalculated results. Where such changes have a significant impact on residual risk outcomes, supervisors should have the option to configure the System to generate alerts or warnings.	Desirable Requirement		



2.12	Assessment Algorithm that Automatically Adapts to Changes in Risk Models	R-132	The assessment algorithm must automatically ensure that risk evaluations remain consistent and up to date whenever variables, hierarchies, 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.	Mandatory Requirement		
		R-133	The System must maintain accuracy and efficiency in all recalculations.	Mandatory Requirement		



2.13	Enhancing ML/FT Risk Detection through Machine Learning.	R-134	The System should include integrated machine learning (ML) and artificial intelligence (AI) capabilities that learn from historical data to improve the accuracy of risk prediction. It must provide predictive analytics to assess current risks and forecast future risks based on past data and observable trends.	Desirable Requirement	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)
------	--	-------	---	-----------------------	--



		R-135	In addition, the System should expose a structured, queryable database and open APIs to ensure compatibility with external AI/ML tools (e.g., offline GPT models) that may be procured separately by the supervisory authority.	Desirable Requirement	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.	R-136	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.	Mandatory Requirement		For example, models for banks, credit organizations, and insurance companies.
		R-137	It should be able to manage and organize any number of financial institutions within each sector.	Mandatory Requirement		
2.15	Building New Risk Models or Customizing Existing Ones	R-138	The System should allow users to create new risk models based on specific parameters such as geography or regulatory requirements.	Mandatory Requirement		
		R-139	The System should be able to integrate existing risk models, ensuring a smooth transition or upgrade without losing previously developed frameworks or methodologies.	Mandatory Requirement		
		R-140	Users should be able to customize the models based on new data or evolving risk assessment needs, ensuring that	Mandatory Requirement		



			risk management processes remain up to date and scalable.			
2.16	Ability to Update Incorrect Data Points	R-141	The System must allow users to identify data points that may be incorrect.	Mandatory Requirement		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.
		R-142	Users should be able to select those data points for correction.	Mandatory Requirement		
		R-143	Only authorized users (e.g., administrators or data managers) should have the ability to update data points.	Mandatory Requirement		
2.17	Roles and Permissions	R-144	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	Mandatory Requirement		



			(Segregation of Duties), and Least Privilege.			
		R-145	The System must support a four-eyes approval process for all re-entries related to changes in inherent risk and control/management quality.	Mandatory Requirement		
		R-146	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.	Mandatory Requirement		
<u>3</u> <i>Data Analysis Capabilities</i> - - - - -						



3.1	Aggregated Statistical Data for Financial Institutions and Sectors	R-147	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.	Mandatory Requirement		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.
		R-148	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.	Mandatory Requirement		
3.2	Changes from the Previous Reporting Period, Data Trend Analysis	R-149	The System must detect and record changes between current and previous reporting cycles. These changes may include:	Mandatory Requirement		Example: If a financial institution's risk rating has



			Differences in indicators, both quantitative and qualitative (e.g., increases or decreases in scores)	Mandatory Requirement		decreased compared to the previous cycle, the System must highlight the change and quantify the difference.
			Changes in risk assessments, thresholds, or other performance indicators	Mandatory Requirement		
			Differences in responses to specific questions or surveys	Mandatory Requirement		Example: A user may wish to compare only high-risk ratings between reporting cycles.
			Institution-specific changes, such as transaction volumes or compliance levels	Mandatory Requirement		
		R-150	Users must be able to view these changes through comparative reports or dashboards.	Mandatory Requirement		Example: A bank may use trend analysis to observe the increase in high-risk transactions over the past six
		R-151	The System must support trend analysis for any defined data metric (e.g., risk scores, transaction volumes, compliance violations) over a selected time period.	Mandatory Requirement		



					months to detect AML/CFT risks.
		R-152	The System must generate visual representations of metric changes, including line charts, bar charts, or other suitable visualizations.	Mandatory Requirement	Example: A financial institution may monitor trends in large cash deposits on a monthly, quarterly, or other time basis.
		R-153	Metric selection: Users must be able to select which metrics to analyze, and the System should allow comparisons between different metrics.	Mandatory Requirement	
		R-154	The System must support bothThe System must support customizable metrics for risk assessment models. Supervisors must be able to build user-defined metrics from scratch, modify or extend uploaded predefined metrics (e.g., risk ratings, transaction volume), and import templates or shared models prepared by the vendor or other supervisory authorities.	Mandatory Requirement	Example: The System should show that the peak in high-value transactions occurred in the first quarter of the year.



		R-155	Timeframe customization: Users must be able to select the analysis period—daily, weekly, monthly, quarterly, or yearly comparisons.	Mandatory Requirement		
		R-156	Trend analysis indicators: The System must calculate key indicators for trend analysis, including:	Mandatory Requirement		
			Percentage changes over time	Mandatory Requirement		
			Moving averages to smooth short-term fluctuations	Desirable Requirement		
			Rate of increase or decrease	Mandatory Requirement		
			Detection of peaks and troughs in the data	Desirable Requirement		
		R-157	Visual and tabular reports: The System must generate both visual reports (e.g., graphs, charts) and tabular reports showing data values over time.	Mandatory Requirement		



		R-158	Users must be able to export these reports in various formats, such as Excel, PDF, or CSV.	Mandatory Requirement		
		R-159	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.	Mandatory Requirement		
3.3	Threshold Definition	R-160	The System must support the selection, storage, and application of thresholds for key ML/FT risk indicators.	Mandatory Requirement		
		R-161	Users must be able to define and reuse customized AML/CFT thresholds.	Mandatory Requirement		
		R-162	The System must allow supervisors to define and configure custom monitoring thresholds.	Mandatory Requirement		
		R-163	When such thresholds are breached, the System must report which should be visible in the supervisory dashboard. These alerts must be	Desirable Requirement		



			distinct from the model's scoring thresholds, and should cover conditions such as absolute value breaches, historical maxima being exceeded, significant percentage changes, or user defined composite rules. All alerts must be recorded in the audit trail.			
3.4	Dashboards on Sector-Specific and Sector Summary Statistical Data	R-164	<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.	Mandatory Requirement		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
		R-165	They should highlight regulatory compliance, emerging risks, or opportunities for improvement.	Mandatory Requirement		
		R-166	They should deliver summary statistical data, such as overall risk levels within the sector.	Mandatory Requirement		



		R-167	This information should be presented in visual formats (charts, tables, or graphs) to simplify data interpretation and facilitate understanding of complex datasets.	Mandatory Requirement		sanctions compliance risks, or their recent increase.
		R-168	Summary dashboards should allow users to compare performance across different financial institutions or sectors, helping identify patterns or deviations.	Mandatory Requirement		
		R-169	<i>Customizable Views:</i> Supervisors should be able to frequently personalize the dashboards to focus on specific metrics, timeframes, or areas of interest.	Mandatory Requirement		
		R-170	<i>Higher frequency data:</i> These dashboards should be able to display near real-time monitoring data (e.g., monthly, weekly, or daily uploads) alongside planned supervisory cycle (quarterly) data. This functionality will enable supervisors to respond quickly	Mandatory Requirement		



			to significant changes in sector performance or risk levels, while maintaining the stability and integrity of the scheduled AML/CFT risk assessment cycle.			
3.5	Horizontal Comparison of Ratings, Responses, and Rankings Across Multiple Financial Institutions.	R-171	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.	Mandatory Requirement		Example:
		R-172	The comparison should include ratings (e.g., risk scores, compliance ratings), responses from surveys or assessments, and rankings, allowing users to see which institution performs best or worst in each category.	Mandatory Requirement		Banking sector: The regulatory authority should be able to compare the risk ratings of different banks side by side to understand which
		R-173	Users should be able to customize the criteria or indicators being compared to align with their operations or regulatory requirements.	Mandatory Requirement		



		R-174	The System should allow users to filter and sort results, focusing on specific sectors, timeframes, or types of responses.	Mandatory Requirement		institutions are the most effective in risk management.
		R-175	Comparisons should be frequently presented in visual formats (charts, tables, graphs), enabling users to quickly identify patterns or deviations across institutions.	Mandatory Requirement		

7. ARCHITECTURAL REQUIREMENTS

No.	Requirement	ID	Description	Critical Requirement	Delivery approach	Examples
	-	-	-	-	-	-
1	Operating System: Windows Server 2019 or later is preferred	R-176	It is desirable for the System to run smoothly on Windows Server 2019 or later versions. The System must not	Mandatory Requirement		



			use outdated or vulnerable protocols (e.g., SMBv1, TLS 1.0/1.1).			
2	Database Requirement (DBMS): Preferably MS SQL Server	R-177	The System must be connected to at least one of the following databases (DBMS): MS SQL Server, Oracle (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).	Mandatory Requirement		
3	Integrated with a flexible monitoring system	R-178	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.	Mandatory Requirement		



4	System recovery tools	R-179	In case of necessary access, users must be able to recover any lost system information. The System must be integrated with Veeam software.	Mandatory Requirement		
5	System management tools	R-180	System management tools should be fully accessible (user registration, assigning user permissions, user replacement, directory maintenance).	Mandatory Requirement		
6	System performance assurance tools	R-181	The Vendor must provide system performance assurance tools, including monitoring and alerting capabilities (e.g., memory usage, storage capacity, system errors, and uptime), to ensure the solution operates reliably and in accordance with agreed performance standards.	Mandatory Requirement		
7	Integration capabilities	R-182	Integration capabilities should include the use of any of the following architectures: Client/Server, N-tier, middleware architecture, and service-oriented architecture (SOA).	Mandatory Requirement		



8. REQUIRED FUNCTIONS FOR SYSTEM ADMINISTRATION, INTEGRATION, AND MANAGEMENT

No.	Requirement	ID	Description	Critical Requirement	Delivery approach	Examples
	-	-	-	-	-	-
1	The software should enable the segregation of user access rights/roles.	R-183	(a) User access roles/permissions are entered into the System for the purpose of user and role management.	Mandatory Requirement		Example: A new supervisor receives access from Active Directory (AD) to general and function-specific processes in accordance with his/her responsibilities.
		R-184	(b) The specified information can be entered into the System either manually or through automated queries from other systems (e.g., AD, SSO, etc.).	Mandatory Requirement		
		R-185	(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	Mandatory Requirement		



			user performing actions or changes in the System (principle of non-repudiation).			
2	All user actions within the System must be logged.		<i>Ability to log user actions within the process. Specifically:</i>			
		R-186	1. The System must retain logs of all user login and registration activities to support security monitoring and anomaly detection.	Mandatory Requirement		
		R-187	2. The System must enforce a Password Policy to ensure the use of strong and regularly updated passwords.	Mandatory Requirement		
3	The System should maintain an audit log of all file exports.	R-188	(a) The audit log must include export activities, including the user who performed the export, and the date and time of the export.	Mandatory Requirement		Example: If a user downloads a file from the System, a unique signature or the user's full
		R-189	(b) Files exported from the System must contain sufficient information to identify the exporting user. If any	Mandatory Requirement		



			such information is modified, the file must become invalid/corrupted.			name is attached to the file.
		R-190	(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 prevention of unauthorized modifications.	Mandatory Requirement		
4	The System should provide functional capability for event log management.	R-191	(a) Functional capability for logging and monitoring predefined System events (including errors and limitations encountered during operation).	Mandatory Requirement		
		R-192	(b) Error categorization and assignment to different administrator groups.	Mandatory Requirement		



5	The System should include management and monitoring window.	R-193	The System must provide real-time visibility into performance and availability information, including metrics such as memory usage, CPU load, storage capacity, API health, and uptime. These metrics must be accessible through an administrative dashboard and exposed via standard interfaces (e.g., logs, APIs) for integration with CBA's monitoring and SIEM tools.	Mandatory Requirement		Example: Real-time graphical representation of performance and errors.
6	The System must support the following technologies/protocols for integration with external systems.	R-194	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:	Mandatory Requirement		
		R-195	API protocols (REST, SOAP, RPC)	Mandatory Requirement		



		R-196	SFTP , HTTPS	Mandatory Requirement		
		R-197	Direct access to databases using any technology	Mandatory Requirement		
		R-198	MQ technologies	Desirable Requirement		
7	The system must support the following data exchange formats	R-199	XLSX or JSON.	Mandatory Requirement		

9. SYSTEM PERFORMANCE AND USER INTERFACE REQUIREMENTS

No.	Requirement	ID	Description	Critical Requirement	Delivery approach	Examples
	-	-	-	-	-	-
1	Ensuring fast and uninterrupted service for at least 10 users simultaneously (maximum capacity: 50 users).	R-200	Uninterrupted operation and System accessibility for concurrently active users.	Mandatory Requirement		



2	The System should be scalable to efficiently process large-volume files without any deterioration in performance.	R-201	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.	Mandatory Requirement		
3	The System should be browser-independent and accessible to users across various devices and platforms.	R-202	Multi-browser compatibility: The System should be compatible with all major web browsers, including Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari, and others.	Mandatory Requirement		



4	The System should be capable of supporting the assessment of a large number of sectors and financial institutions at least on a quarterly basis.	R-203	The System must support quarterly AML/CFT risk assessments as the formal supervisory cycle, providing a stable basis for supervisory planning and the setting of priorities (17 banks, 42 credit organizations, 16 payment and settlement organizations, 22 investment companies, and 1 depository). At the same time, the System must also support higher-frequency inherent risk estimations for monitoring purposes (e.g., monthly, weekly, or daily), in order to take into account significant changes at the institutional or sector level between assessment cycles. This dual approach will allow supervisors to maintain a consistent, comprehensive cycle for engagement planning while also benefiting from dynamic monitoring capabilities to detect emerging risks and support timely interventions.	Mandatory Requirement		
---	--	-------	---	-----------------------	--	--



5	The System should be user-friendly and easy to navigate for all users.	R-204	Easy and Intuitive Navigation – The System structure should allow users to quickly find the required functionality without extensive searching.	Mandatory Requirement		
		R-205	User Journey Clarity – The UI/UX design should ensure that users clearly understand their next steps and can easily perform the required actions.	Mandatory Requirement		
		R-206	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.	Mandatory Requirement		
		R-207	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.	Mandatory Requirement		



10. SYSTEM SECURITY REQUIREMENTS

No.	Requirement	ID	Description	Critical Requirement	Delivery approach	Examples
	-	-	-	-	-	-
1	The System should ensure the security of data exchange between the user and the server.	R-208	The System should ensure secure data transmission between the user and the server, preventing data leakage, unauthorized access, and cyber threats.	Mandatory Requirement		
2	Compliance with international security standards	R-209	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:	Mandatory Requirement		
		R-210	8.25 – Secure development life cycle	Mandatory Requirement		



		R-211	8.26 – Application security requirements	Mandatory Requirement		
		R-212	8.27 – Secure System architecture and engineering principles	Mandatory Requirement		
		R-213	8.28 – Secure coding	Mandatory Requirement		
		R-214	8.29 – Security testing in development and acceptance	Mandatory Requirement		
		R-215	8.30 – Outsourced development	Mandatory Requirement		
3	The System should provide the ability to set limitations on attachments, including size, format, and other relevant criteria.	R-216	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.	Mandatory Requirement		
4	System Disaster Recovery Plan	R-217	The System should ensure automatic backup, data recovery, uninterrupted operation during emergency situations, and rapid restart mechanisms (Failover & Failback). It	Mandatory Requirement		



			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.	R-218	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.	Mandatory Requirement		
		R-219	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.	Mandatory Requirement		



6	Security and Authentication	R-220	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).	Mandatory Requirement		
		R-221	Integration with Advanced MFA Solutions: The System should also 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.	Mandatory Requirement		
		R-222	Role-Based Access Control (RBAC): The System should enforce role-based access control to restrict access to data and System functionalities based	Mandatory Requirement		



			on the user's assigned role. This minimizes the risk of unauthorized access and data misuse.			
		R-223	User Activity Logging and Monitoring: The System should maintain comprehensive logs of user activities, including login attempts, data modifications, and other critical actions.	Mandatory Requirement		
		R-224	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.	Mandatory Requirement		



7	Business Continuity	R-225	Redundancy: The System should support redundancy across key components (e.g., servers, databases, storage) to eliminate single points of failure. The Vendor is responsible for ensuring that the application layer is fully compatible with CBA's high-availability infrastructure, providing the necessary configuration guidelines, and validating through testing that in the event of a component failure, redundant components automatically assume operations to ensure uninterrupted service.	Mandatory Requirement		
---	---------------------	-------	---	-----------------------	--	--



		R-226	Monitoring and Alerts: The System must include built-in application-level monitoring and alerting mechanisms (e.g., service status, error logs, API health, job execution, and data processing) to help administrators detect and respond to potential issues before they cause disruptions. The Vendor must ensure that the System is fully compatible with CBA's existing monitoring and SIEM tools by exposing the necessary logs, metrics, and APIs for integration.	Mandatory Requirement		
--	--	-------	--	-----------------------	--	--

11.AUDITABLE REQUIREMENTS

No.	Requirement	ID	Description	Critical Requirement	Delivery approach	Examples
-	-	-	-	-	-	-



1	Unsuccessful login attempts	R-227	The System should restrict the number of consecutive invalid login attempts by a user.	Mandatory Requirement		
		R-228	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.	Mandatory Requirement		
2	Session termination	R-229	The System should automatically terminate a user session after a defined period of inactivity.	Mandatory Requirement		
3	Automated labeling	R-230	The System should use standardized labeling templates to tag outgoing data in order to identify any special	Mandatory Requirement		



			instructions for dissemination, processing, or distribution.			
4	Auditable Events		<i>The System should generate audit logs for the following events:</i>			
		R-231	Creation, activation, modification, review, deactivation, and deletion of user accounts	Mandatory Requirement		
		R-232	Creation and modification of protected objects, and access to them	Mandatory Requirement		
		R-233	Login and logout events	Mandatory Requirement		
		R-234	Unsuccessful login and access attempts	Mandatory Requirement		
5	Audit Log Content	R-235	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:	Mandatory Requirement		
		R-236	Date and time of the event	Mandatory Requirement		



		R-237	System component involved	Mandatory Requirement		
		R-238	Type of event	Mandatory Requirement		
		R-239	Identity of the user/entity	Mandatory Requirement		
		R-240	Outcome/result of the event (success or failure)	Mandatory Requirement		
		R-241	The System should allow the inclusion of additional, more detailed information in audit logs based on event type, location, or entity involved.	Mandatory Requirement		
		R-242	The System should enable centralized management of the content of audit logs generated by individual components across the entire System.	Desirable Requirement		
6	Response to Audit Process Failures	R-243	In the event of audit process failures, the System should notify the relevant authorized personnel within the organization.	Mandatory Requirement		



		R-244	Audit process failures may include, for example: software/hardware errors, failures in the audit logging mechanism, and exceeding or exhausting audit storage capacity	Mandatory Requirement		
		R-245	The System should issue a warning when the allocated storage for audit logs approaches a defined threshold.	Mandatory Requirement		
7	Audit Log Reduction and Report Generation	R-246	The System should provide the capability to reduce the volume of audit logs and generate reports	Mandatory Requirement		
		R-247	The System should support the automated processing of audit records related to events of interest, based on configurable event criteria.	Mandatory Requirement		
8	Protection of Audit Information	R-248	The System should ensure the protection of audit information and audit tools from unauthorized access, modification, and deletion.	Mandatory Requirement		
9	Non-repudiation	R-249	The System should provide the ability to determine whether a specific	Mandatory Requirement		



			individual has performed a particular action.			
10	Minimum Functionality	R-250	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.	Mandatory Requirement		
11	Transmission Integrity	R-251	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.	Mandatory Requirement		
12	Transmission Confidentiality	R-252	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.	Mandatory Requirement		



13	Data Confidentiality and Protection	R-253	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.	Mandatory Requirement		
		R-254	The Vendor is strictly prohibited from disclosing, processing, transferring, copying, or otherwise using any real supervisory data for testing or development purposes.	Mandatory Requirement		
		R-255	For system testing, only anonymized and artificial (“dummy”) data, generated or approved by the Client, shall be used.	Mandatory Requirement		
		R-256	The CBA AML/CFT risk assessment methodology, supervisory models, scoring frameworks, and related	Mandatory Requirement		



			intellectual property must be treated as strictly confidential information.			
		R-257	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.	Mandatory Requirement		
		R-258	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.	Mandatory Requirement		
		R-259	The Vendor shall be required to sign a Data Confidentiality and Non-Disclosure Agreement (NDA) prior to any access to the system environment.	Mandatory Requirement		



14	Security Testing and Risk Assessment	R-260	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.	Mandatory Requirement		
15	Data Deletion	R-261	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.	Mandatory Requirement		
16	Accuracy, Completeness, Validity, and Authenticity of Information	R-262	The System should verify the accuracy, completeness, validity, and authenticity of information.	Mandatory Requirement		



17	System Component Inventory	R-263	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.	Mandatory Requirement		
		R-264	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.	Mandatory Requirement		
		R-265	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.	Mandatory Requirement		



18	System Recovery and Reconfiguration	R-266	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.	Mandatory Requirement		
19	System Maintenance Policy and Procedures	R-267	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.	Mandatory Requirement		
20	Timely Maintenance	R-268	The applicant shall provide maintenance and support for an agreed-upon period.	Mandatory Requirement		



21	System Documentation	R-269	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.	Mandatory Requirement		
22	Configuration and Change Management	R-270	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.	Mandatory Requirement		
23	Third-Party License	R-271	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	Mandatory Requirement		



			or assume any related legal, financial, or technical responsibilities.			
--	--	--	--	--	--	--

12. GENERAL TECHNICAL REQUIREMENTS

No.	Requirement	ID	Description	Critical Requirement	Delivery approach	Examples
	-	-	-	-	-	-
1	The programming code used in the System shall be based on the latest available versions.	R-272	The System's source code, databases, and programming frameworks must utilize the latest available stable versions.	Mandatory Requirement		
		R-273	All System components must currently be supported by their respective vendors.	Mandatory Requirement		
		R-274	Discontinued or obsolete technologies must not be used.	Mandatory Requirement		
		R-275	The use of software that has reached End of Life (EOL) or End of Support (EOS), as officially declared by the	Mandatory Requirement		



			vendor or development group, is strictly prohibited.			
		R-276	Software not receiving security updates must be replaced or updated with appropriate alternatives.	Mandatory Requirement		
		R-277	The Bidder shall ensure that the proposed solution operates as an integrated system, with all software components fully compatible and interoperable within the overall System architecture and operating environment.	Mandatory Requirement		
		R-278	Third-party software must be backed by long-term support (LTS) guarantees.	Mandatory Requirement		
2	The vendor shall submit a System implementation plan.		The implementation plan shall include, at a minimum, the following:			
		R-279	A schematic diagram of the System components' integration and installation	Mandatory Requirement		



		R-280	A description of network connections	Mandatory Requirement		
		R-281	A description of data flows, <i>refer to Figure 1</i>	Mandatory Requirement		
		R-282	Configuration files and their descriptions	Mandatory Requirement		
		R-283	A list and description of third-party/vendor-provided resource components and their required capacities necessary for System maintenance and operational continuity.	Mandatory Requirement		
3	The vendor, with the participation of the client's specialists, shall configure the "Testing Environment" and "Production Environment."	R-284		Mandatory Requirement		



13. TRAINING AND EDUCATIONAL MATERIALS

No.	Requirement	ID	Description	Critical Requirement	Delivery approach	Examples
	-	-	-	-	-	-
1	The Vendor shall provide all necessary user guides and reference materials to ensure effective use of all System components.	R-285	User manual: A detailed user manual must be provided, explaining the core functionality of the System. It should include step-by-step instructions, navigation guides, and troubleshooting tips.	Mandatory Requirement		
		R-286	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.	Mandatory Requirement		
		R-287	Training program: A training program must be provided alongside the System, detailing course topics and materials, covering both basic user	Mandatory Requirement		



			training and advanced risk modeling techniques.			
		R-288	First-line support guidelines: A first-line support guide must be provided, including general troubleshooting steps and processes, including:	Mandatory Requirement		
		R-289	Basics of System error resolution	Mandatory Requirement		
		R-300	Frequently asked questions (FAQ) and answers to common user issues	Mandatory Requirement		
		R-301	Instructions on escalating issues to higher-level support	Mandatory Requirement		
		R-302	Technical operation manual: A manual for System operators and administrators, including regular maintenance schedules, data archiving, recovery mechanisms, backup replication, troubleshooting, and more.	Mandatory Requirement		



		R-303	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:	Mandatory Requirement		
		R-304	A comprehensive list of API endpoints	Mandatory Requirement		
		R-305	Authentication protocols and mechanisms	Mandatory Requirement		
		R-306	Definitions of input/output data formats	Mandatory Requirement		
		R-307	Sample requests and responses	Mandatory Requirement		
		R-308	Rate limiting and error handling policy	Mandatory Requirement		
		R-309	Technical limitations	Mandatory Requirement		
2	System Administrator Guide	R-310	The purpose of the program (or System) and its scope of application,	Mandatory Requirement		



	R-311	The structure of the program, its operational principles,	Mandatory Requirement		
	R-312	The delivery package (if not specified in a separate document),	Mandatory Requirement		
	R-313	The System requirements for the program or its components,	Mandatory Requirement		
	R-314	The preferred installation sequence of the components,	Mandatory Requirement		
	R-315	The installation process for the program or each of its components,	Mandatory Requirement		
	R-316	The mandatory configuration sequence for the program,	Mandatory Requirement		
	R-317	The integration methods for the installed copies of the components,	Mandatory Requirement		
	R-318	The integration of the program, e.g., with software, database server,	Mandatory Requirement		
	R-319	Methods and frequency of verifying the accuracy of program operation,	Mandatory Requirement		
	R-320	The current maintenance procedure for the active program copies,	Mandatory Requirement		



		R-321	The process for resolving any potential support issues,	Mandatory Requirement		
		R-322	Emergency situations and the methods for overcoming them,	Mandatory Requirement		
		R-323	User interface for the administrative panel,	Mandatory Requirement		
		R-324	Command-line interface tools and their execution sequence,	Mandatory Requirement		
		R-325	Configuration files and their writing rules,	Mandatory Requirement		
		R-326	The scripting language for writing control scripts.	Mandatory Requirement		
3	User/Technical Team Training	R-327	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	Mandatory Requirement		



			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.	R-328	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.	Mandatory Requirement		

14.TESTING/VALIDATION

No.	Requirement	ID	Description	Critical Requirement	Delivery approach	Examples
	-	-	-	-	-	-
1	Deployment validation		<i>The Vendor shall:</i>			



	R-329	Provide all relevant documentation (see TRAINING AND EDUCATIONAL MATERIALS for details), including the deployment verification checklist, configuration, and integration documentation.	Mandatory Requirement		
	R-330	Deliver, configure, and provide all necessary technical support to the Client during the integration process of features available in the solution and ensuring compatibility with the Client's systems.	Mandatory Requirement		
	R-331	Assist the Client in enabling connectivity to internal and external systems by providing guidance, technical support, and professional services where required.	Mandatory Requirement		
		<i>The Client shall:</i>			



	R-332	Provide the necessary environment, including network access, security approvals, test environments and any other prerequisites required for system configuration and integration.	Mandatory Requirement		
	R-333	Perform system configuration based on the documentation provided by the Vendor, in alignment with supervisory business logic and risk methodology.	Mandatory Requirement		
	R-334	Perform the integration work, while the Vendor must fully support and assist the Client's team without charging any additional fees for integration-related support.	Mandatory Requirement		
	R-335	Confirm that network and integration points are functioning as intended.	Mandatory Requirement		
	R-336	Review and approve the submitted documentation.	Mandatory Requirement		



		R-337	Formally confirm readiness to proceed to acceptance testing only after successful deployment validation.	Mandatory Requirement		
			<i>Deployment validation is considered successful (pass) if:</i>			
		R-338	All system components are operational and accessible.	Mandatory Requirement		
		R-339	Information security and integration are verified.	Mandatory Requirement		
		R-340	Configuration aligns with supervisory requirements.	Mandatory Requirement		
		R-341	No outstanding technical issues remain.	Mandatory Requirement		
		R-342	All required documentation is submitted and approved by the Client.	Mandatory Requirement		
2	Acceptance Testing (QA + UAT) — In Line with ISO/IEC 12207 and ISO/IEC 90003	R-343	The Vendor shall submit a testing plan, including a test guide and acceptance criteria, enabling the evaluation of whether the deployed	Mandatory Requirement		



		system meets the Client's business, functional, performance, security, and usability requirements, based on real supervisory scenarios and test cases.			
		<i>Vendor Responsibilities</i>			
	R-344	Support the Client throughout the testing phase by:	Mandatory Requirement		
	R-345	Assisting in the logging and classification of defects	Mandatory Requirement		
	R-346	Ensuring timely resolution of bugs and correction of defects	Mandatory Requirement		
	R-347	Track all issues in a defect Log, including status, severity, resolution date, and retesting outcome.	Mandatory Requirement		
	R-348	Upon completion of testing, provide a summary report covering test coverage and identified issues.	Mandatory Requirement		
		<i>Client Responsibilities</i>			



	R-349	Provide a fully operational test environment aligned with the production configuration.	Mandatory Requirement		
	R-350	Execute test scenarios that reflect real supervisory use cases (e.g., risk scoring validation).	Mandatory Requirement		
	R-351	Review outputs such as dashboards, alerts/red flags, and reports for accuracy and compliance.	Mandatory Requirement		
	R-352	Log all results and defects using the pre-agreed classification methodology (e.g., Critical, High, Medium, Low).	Mandatory Requirement		
	R-353	Validate key non-functional aspects, including system performance, authorized access, and usability.	Mandatory Requirement		
	R-354	Confirm whether each requirement has been met based on predefined acceptance criteria (e.g., expected scores, accuracy of workflows, compliance of reports).	Mandatory Requirement		



			<i>Testing is considered "Accepted" (pass) if:</i>	Mandatory Requirement		
		R-355	All business scenarios operate fully and correctly without errors or defects.	Mandatory Requirement		
		R-356	No unresolved bugs or deficiencies remain.	Mandatory Requirement		
		R-357	Value attributes such as functionality, performance, usability, security, and integration are confirmed.	Mandatory Requirement		
		R-358	All test documentation, defect logs, and resolution reports are reviewed and approved by the Client.	Mandatory Requirement		
3	Defect classification and resolution during acceptance testing (QA + UAT)	R-359	Each defect logged during acceptance testing must be classified by severity:	Mandatory Requirement		
		R-360	Critical – Blocks essential System functionality (e.g., incorrect risk scoring, failed data import),	Mandatory Requirement		



	R-361	High – Impacts core business workflows (e.g., incorrect escalation of alerts/red flags, non-functional dashboards),	Mandatory Requirement		
	R-362	Medium / Low – Non-blocking user interface bugs or improvement suggestions,	Mandatory Requirement		
		<i>Defect resolution: The Vendor is responsible for:</i>			
	R-363	Applying technical fixes	Mandatory Requirement		
	R-364	Optimizing configurations and parameters	Mandatory Requirement		
	R-365	Updating APIs or integration components as needed	Mandatory Requirement		
		<i>Retesting and closure process</i>			
	R-366	After fixes are deployed, the Client must retest the failed scenario(s) to confirm the issue has been resolved.	Mandatory Requirement		



		R-367	Closure is permitted only after the Client confirms resolution and successful retest results are documented.	Mandatory Requirement		
			<i>The defect resolution phase is considered successfully completed (Passed) when:</i>			
		R-368	All defects are closed and approved by the Client	Mandatory Requirement		
		R-369	No new issues have emerged during retesting	Mandatory Requirement		
		R-370	All defects and resolutions are fully documented	Mandatory Requirement		
		R-371	The updated Defect Log is approved by the Client	Mandatory Requirement		
4	Pilot operation	R-372	The pilot phase should focus on validating the operational supervisory workflows using real data. The following key components are typically included:	Mandatory Requirement		



	R-373	Risk scoring logic and alert thresholds	Mandatory Requirement		
	R-374	Generation of red flags and supervisory dashboards	Mandatory Requirement		
	R-375	Visualization and report generation	Mandatory Requirement		
	R-376	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.	Mandatory Requirement		
		<i>The Pilot Phase is considered successful ("Accepted") if:</i>			
	R-377	Supervisory users are able to complete end-to-end workflows without obstacles or failures	Mandatory Requirement		
	R-378	No logic errors or system crashes occur during run	Mandatory Requirement		



		R-379	Users confirm that key value attributes (e.g., functionality, usability, risk scoring, navigation) are satisfactorily met	Mandatory Requirement		
5	Go-Live Readiness Sign-Off	R-380	The following phases must be fully completed and approved before Go-Live Readiness can be confirmed:	Mandatory Requirement		
		R-381	Deployment Validation	Mandatory Requirement		
		R-382	All system modules are deployed, configured, and accessible	Mandatory Requirement		
		R-383	User Acceptance Testing (QA + UAT)	Mandatory Requirement		
		R-384	All functional and non-functional requirements are verified	Mandatory Requirement		
		R-385	Defect Resolution	Mandatory Requirement		
		R-386	All issues are resolved and formally closed	Mandatory Requirement		



	R-387	Pilot Run	Mandatory Requirement		
	R-388	Critical/core workflows are demonstrated by real end-users	Mandatory Requirement		
	R-389	Successful Implementation of the CBA AML Methodology	Mandatory Requirement		
	R-390	The AML/CFT risk assessment methodology defined by the Central Bank of Armenia (CBA) is fully implemented, tested, and validated within the System.	Mandatory Requirement		
	R-391	Training Completion (<i>see Chapter 13 for details</i>)	Mandatory Requirement		
	R-392	End-user training conducted for supervisors, analysts, and administrators	Mandatory Requirement		
	R-393	Documentation Delivered	Mandatory Requirement		
	R-394	System and Technical Architecture Documentation, Configuration Summaries, API Documentation,	Mandatory Requirement		



			Non-Functional Specifications, User Manuals, Standard Operating Procedures (SOPs)			
			<i>Pass Condition:</i>			
		R-395	The Client signs the Go-Live Readiness Certificate, confirming that the solution meets all operational criteria and is ready for production use.	Mandatory Requirement		
			<i>Fail Condition:</i>			
		R-396	Unresolved defects, missing documentation, or open testing gaps prevent the system from going live.	Mandatory Requirement		

15. TECHNICAL SUPPORT AND MAINTENANCE REQUIREMENTS

No.	Requirement	ID	Description	Critical Requirement	Delivery approach	Examples
-	-	-	-	-	-	-



1	The Supplier must provide system maintenance for a period of 5 years.	R-397	Warranty service for a period of 1 year	Mandatory Requirement		
		R-398	Technical maintenance and support for a period of 5 years	Mandatory Requirement		
		R-399	System Updates and Optimization	Mandatory Requirement		
		R-400	Security Support	Mandatory Requirement		
		R-401	User Support and Training	Mandatory Requirement		
		R-402	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).	Mandatory Requirement		
2	Warranty and Operational Support	R-403	The Vendor shall provide a warranty for all solution components delivered within the specified warranty period.	Mandatory Requirement		



		R-404	During the specified warranty period, the Vendor shall act as the Client's agent for requesting repairs or corrections for any part of the System supplied and guaranteed by the Vendor. The System components under warranty — including but not limited to software modules, configuration settings, APIs, user interfaces, integration connectors, and reporting/analytics functions — shall be corrected or restored 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.	Mandatory Requirement		
--	--	-------	--	-----------------------	--	--



		R-405	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). The primary responsibility of this expert will be to diagnose and fix any system issues to restore normal operations. In addition, the expert shall assist the Client's operational team as required.	Mandatory Requirement		
3	Technical support shall be available at three levels.	R-406	First Level (Internal Support provided by the Client): The Vendor shall provide adequate training, together with all necessary documentation to enable the Client's IT personnel to deliver first-level support for the operation of the System. The Client's IT personnel shall be capable of resolving basic	Mandatory Requirement		



			operational issues raised by supervisors.			
		R-407	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.	Mandatory Requirement		
		R-408	Second-Level Technical Support 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	Mandatory Requirement		



			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.			
		R-409	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.	Mandatory Requirement		
		R-410	The Client shall receive consultancy on new features related to the development environment, supporting resources, and related	Mandatory Requirement		



			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.			
		R-411	The Vendor shall provide maintenance services to ensure the continuous and reliable operation of the System. Maintenance shall include corrective, preventive, and adaptive support, delivered primarily via secure remote access. The Vendor shall provide software updates and patches related to functionality, performance, and security at no additional cost. The Vendor shall guarantee timely response and resolution of issues in accordance with agreed service levels (SLA). The Vendor shall also deliver updated documentation and	Mandatory Requirement		



			knowledge transfer for the Client's IT staff as part of maintenance activities.			
4	Documentation Updates	R-412	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.	Mandatory Requirement		
		R-413	All accepted international and industry standards, as well as applicable local standards, must be clearly referenced and accompanied by detailed descriptions of similar standards.	Mandatory Requirement		



		R-414	The Vendor is encouraged, where feasible, to also provide detailed and up-to-date documentation in Armenian.	Desirable Requirement		
		R-415	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.	Desirable Requirement		

16.SYSTEM PRESENTATION REQUIREMENTS

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

17.EXPECTED DELIVERABLES AND PLANNED TIMELINES

The tentative timeline is for guidance only but the final implementation timeline cannot exceed 11 months overall. Participants must submit, in their proposals, a detailed schedule for contract execution, specifying all key phases and their respective target completion dates.



EXPECTED DELIVERABLES	TENTATIVE TIMELINE
Delivery and Deployment of the System - All modules are installed, configured, and integrated.	Up to 6 months
Training Course - End-User Training for Supervisors, Analysts, and Administrators	
User Acceptance Testing (QA + UAT) - All functional and non-functional requirements have been validated.	Up to 3 months
Pilot operation - Critical and key workflows are executed and demonstrated by real users.	Up to 1 months
Final Delivery and Acceptance of the System	Up to 1 months
Technical Support and Maintenance	In line with the timeline provided in the proposal

The Vendor shall provide the Project roadmap and the Project Implementation Timeline.

If necessary, the Vendor must be physically present during the System deployment, acceptance testing, handover-acceptance, and training phases.



18. 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.

Additionally, the Participant shall demonstrate that the proposed solution is a mature Commercial Off-The-Shelf (COTS) product. Evidence must include product documentation confirming that the solution is a standard, fully developed COTS system, along with descriptions of existing COTS deployments in comparable supervisory or regulatory authorities.

Custom development required to address COTS gaps shall not exceed 10% of the Mandatory Functional Requirements. Any proposal exceeding these thresholds may, at the Client's discretion, be considered non-compliant.



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 of system supply and implementation, including the costs of deployment, installation, commissioning, and training, as well as the expected post-warranty expenses over a 5-year period, including maintenance and support costs (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 supply and implementation costs using Annex 3.1, clearly specifying the unit and total prices for each proposed component, including terms, schedule, and procedure for payment.



- 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, such as for staff travel or other necessary expenses and other extended services.
- 2.1.5. The Financial Proposal shall include pricing only for Mandatory requirements. This total will be used for financial evaluation and comparison.
- 2.1.6. Pricing for requirements “Desirable” shall be provided in a separate section or table, clearly itemized (Not Evaluated). Optional pricing shall not be included in the Mandatory pricing total. Such pricing may be considered for future contracting, depending on budget and need.
- 2.1.7. If a Mandatory or Optional requirement is not available in the Bidder’s COTS solution (or Standard Services) but can be developed, configured or provided (Extended Services) at additional cost, the Bidder must clearly indicate this and provide the corresponding price in the Optional/Desirable Pricing and mandatory sections. The Bidder shall also specify the additional time required for such development.
- 2.1.8. The Bidder shall not bundle or incorporate Optional/Desirable requirement costs or development costs into Mandatory pricing.
- 2.1.9. Optional and development pricing shall remain valid for the proposal validity period and may be procured later at the stated prices, and—upon entering into a contract—the quoted optional and development pricing shall remain fixed and valid for an additional 12–24 months, depending on the agreed contract terms.



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. The terms of the system's warranty, as well as its ongoing technical support and maintenance
 - 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 or through other manufacturer-approved service channels. The details of such service centers or authorized service arrangements must be available on the manufacturer's official website or validated through 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).

19.SPECIAL CONDITIONS

1. Requirements Classification and Pricing Rules

Unless explicitly stated otherwise, **all requirements in this Terms of Reference (ToR) are Mandatory.**

Requirements are classified as follows:

- **Mandatory Requirements** - Mandatory Requirements represent the minimum functional, technical, security, and regulatory scope of the Project.
 - ✓ The Bidder **shall fully comply with all Mandatory Requirements**, and **all costs necessary to meet these requirements shall be included in the Implementation Price.**
 - ✓ Notwithstanding the above, where a Bidder proposes a **mature Commercial Off-The-Shelf (COTS) solution**, the Client may, at its sole discretion, accept limited deviations from Mandatory Requirements, subject to the following conditions:
 - the solution may lack compliance with **no more than ten percent (10%) of the Mandatory Requirements**;
 - the missing functionalities shall be **non-critical** and shall **not affect**:
 - regulatory or supervisory compliance,



- data integrity or security, or
 - core ML/FT and sanctions risk assessment and monitoring capabilities;
- the missing functionalities shall be deliverable through **additional development without architectural redesign**; and
- such development shall:
 - be considered part of the implementation,
 - be fully included in the Implementation Price, and
 - be delivered within the proposed implementation timeline.

The Bidder shall **clearly identify** all such deviations in its Technical Proposal.

- **Desirable Requirements**

- ✓ Requirements explicitly marked as “**Desirable**” are not mandatory and shall not affect eligibility or compliance.
- ✓ If a Desirable Requirement:
 - is already available in the proposed solution, it may be included at no additional cost; or
 - requires additional licenses, modules, development, or third-party components, the Bidder shall:
 - clearly describe the scope of such enhancements, and
 - present the corresponding costs exclusively in the Optional Price List of the Proposal.
- ✓ Costs related to Desirable Requirements **shall not be included in the Implementation Price** and shall be evaluated separately.
- ✓ The Client reserves the right to:
 - accept or reject any Optional items, in whole or in part, and
 - contract Optional Requirements separately or not at all, without affecting the award of the main contract.



2. 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.
3. 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.
4. 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.
5. The System implementation date shall be considered the date on which the final acceptance certificate is signed. The warranty period shall commence from the same date.
6. The end of the warranty period shall signify the start of technical support and maintenance services.
7. 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.

20. GENERAL TERMS OF THE CONTRACT

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.
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:

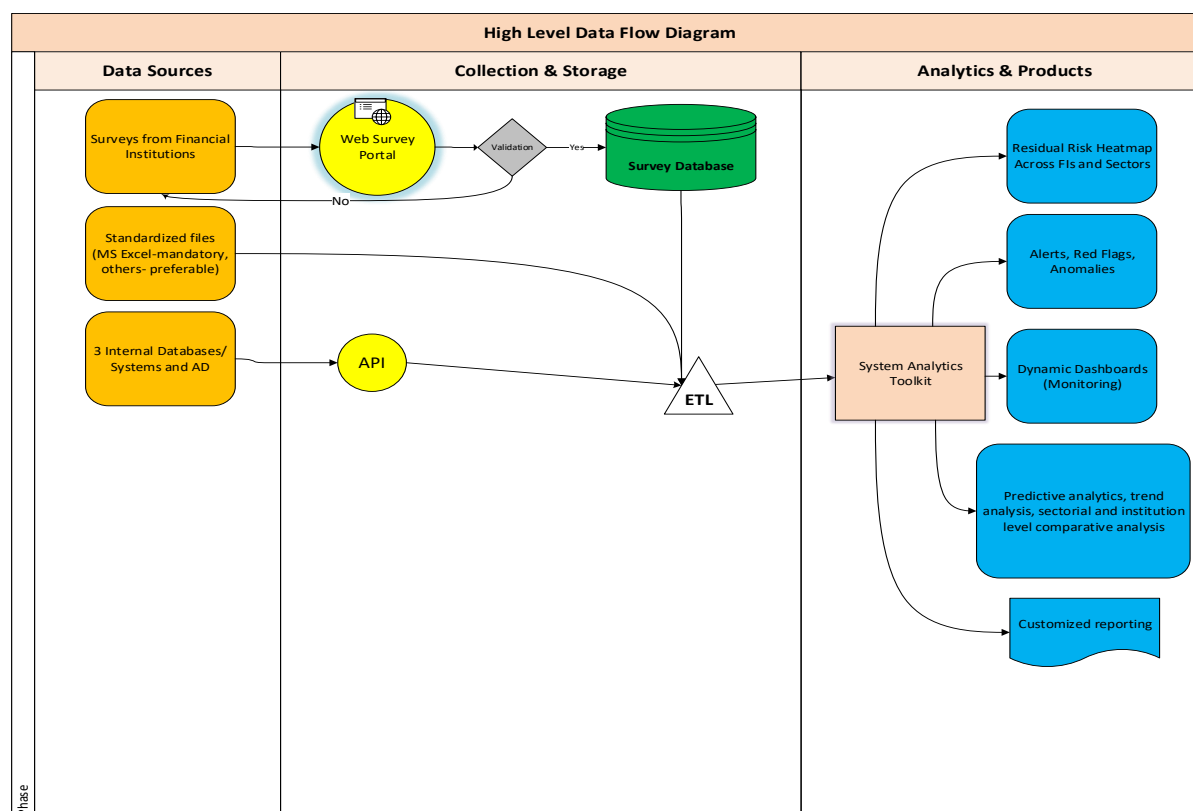


- 3.1. After the implementation of the system (or individual subsystems), the Client shall, within the timeframe defined in the mutually agreed and approved schedule, review the quality of the work performed and its compliance with the requirements specified in the Contract. If no deficiencies are identified, the Client shall sign the relevant acceptance certificate(s).
4. The payment terms and conditions shall be stipulated in the Contract. The provision of technical maintenance and support services, as well as the procedures for acceptance, handover, and payment following system implementation, shall be defined in the Contract.
5. 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 only**, and **shall be calculated solely based on the value of the delayed or unperformed portion of the work**, subject to the legally established maximum annual limits.
6. 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.

The Client shall have the right to deduct, without acceptance, any penalties payable by the Contractor **calculated on the basis of the value of the unperformed or delayed services**, from the amounts due to the Contractor under the Contract.

Figure 1

Workflow diagram





№	LIST OF DOCUMENTS	
1.	Application-statement approved by the bidder in accordance with Appendix 2 attached to this Invitation	☐
2.	A document confirming the bid security for participation in the tender	☐
3.	The financial proposal, completed in accordance with Appendix 3 to this Invitation	☐
4.	Breakdown of the financial proposal, completed in accordance with Appendix 3.1 and 3.2, including proposed payment terms and conditions	☐
5.	The technical proposal, including the detailed description of the proposed solution, prepared in accordance with Appendix 4	☐
6.	Company Portfolio, completed in accordance with Appendix 5	☐
7.	Organizational and Governance Overview, completed in accordance with Appendix 6	☐
8.	Any other supporting documents and information specified in Terms of Reference of this Invitation, including those that demonstrate the bidder's capacity, experience, or other qualifications supporting its proposal	☐
9.	A draft version of the contract outlining the principal terms, conditions, responsibilities, and other relevant provisions (if available).	☐



APPLICATION-STATEMENT

Participation in Tender

_____ [Name of Bidder or in case of JV, insert legal name of each member] *
wishes to participate in Lot(s) _____ of the Tender with Reference Number CBA-2026-001 announced by the Central Bank of Armenia and submits a proposal in accordance with the requirements of the Invitation.

We, the undersigned, declare and certify that:

1. We have reviewed the Invitation documents and have no reservations.
2. As of the date of submission of the bid, we meet the eligibility requirements set forth in the Invitation and, in accordance with clause 2.1 of the Invitation,
 - a) We have not been declared bankrupt by a court and are not in the process of liquidation.
 - b) During the previous five years, we have not been convicted of a crime involving the financing of terrorism, child exploitation or human trafficking, creating or participating in a criminal partnership, receiving a bribe, giving or brokering a bribe, or crimes against economic activity as prescribed by law, except in cases in which the conviction has been removed or extinguished in a manner prescribed by law.
 - c) We have not allowed and/or will not allow anti-competitive agreements, unfair competition, or abuse of dominant position in the course of our participation in this procedure.
 - d) There is no simultaneous participation of any affiliated persons as defined in the Invitation and/or organizations founded by us or in which we hold more than a fifty percent share.

Moreover, the declaration regarding actual beneficiaries is submitted in accordance with Appendix 2.1.

* In the case of submitting a Proposal in the form of joint activity (consortium), the application declaration must be submitted by all members of the consortium.



- e) We are not included in the list of bidders who are not eligible to participate in the procurement process published in accordance with the procurement laws of member states of the Eurasian Economic Union.
- f) We are not included in the list of bidders who are not eligible to participate in the procurement process.
3. Our proposal takes effect from the date of the deadline for submission of proposals specified in the announcement and is valid until the event specified in clause 9.4 of the Invitation.
4. If we become a selected bidder, we undertake to provide contract security in accordance with the Invitation and to deliver the services in accordance with the timeframes for provision of the Services specified in the Technical Task.
5. In accordance with clause 3.3 of this Invitation, as a bidder, we are not submitting more than one proposal to this tender process.
6. We understand that this bid, if selected, is a binding contract between us until a formal contract is prepared and executed.

1) Name of Bidder:	<i>[insert Bidder's legal name], or [In case of JV, insert legal name of each member]</i>
2) Legal Address:	<i>[insert Bidder's legal address in country of registration], or [In case of JV, insert legal address in country of registration of each member]</i>
3) Business Address (if different):	<i>[insert Bidder's business address in country of registration], or [In case of JV, insert business address in country of registration of each member]</i>
4) Taxpayer Identification Number:	<i>[insert Bidder's Taxpayer identification number] or [In case of JV, insert Taxpayer identification number of each member]</i>
5) Phone Numbers:	
6) E-mail Address:	
7) Website:	
8) First Name and Last Name, Position, and Contact Information for Authorized Representative of Bidder:	



Copies of the following original documents are attached:

- ☐ Organization Registration Documents
- ☐ In the case of a joint venture, the JV agreement

First Name and Last Name of Bidder's Principal:	
Position of Bidder's Principal:	
Signature of Above-Named Person	
Signing Date:	



DECLARATION REGARDING ACTUAL BENEFICIARIES

Information About Organization		
1.	Name	
2.	Registered/Legal Address	
3.	Business Address (if different)	
4.	Phone Number	
5.	E-mail Address	
6.	Website	
7.	First Name, Last Name, Position, Phone Number, and E-mail Address of Person Submitting the Declaration	
8.	First Name, Last Name, Position, Phone Number, and E-mail Address of Head(s) of Executive Body (with authority to sign in accordance with bidder's formation (charter) documents)	
9.	As of the date of submission of the bid, is the organization included in the list of persons not entitled to participate in the procurement process?	Yes ☐ No ☐
OWNERSHIP TYPE AND COMPOSITION OF OWNERS		
10.	Co-Founded	Yes ☐ No ☐
	If yes, provide details, including information about shareholders holding 20% or more of the shares.	



	First Name, Last Name/Name	Citizenship/Country of Registration	Date of Birth/ Date of State Registration	Passport Series, Number/ State Registration Number	Amount of Share Ownership
	Private		Yes ☐ No ☐		
	If yes, provide information about shareholders holding 20% or more of the shares.				
	First Name, Last Name/Name	Citizenship/Country of Registration	Date of Birth/ Date of State Registration	Passport Series, Number/ State Registration Number	Amount of Share Ownership
INFORMATION ABOUT EXECUTIVE BODY					
	Provide information about the members of the organization's executive body.				
11.	First Name, Last Name	Citizenship	Date of Birth	Passport Series, Number	Position
PERSONS WITH POLITICAL INFLUENCE[†]					
12	Are there any persons with political influence among the owners or the executive body of the organization?		Yes ☐ No ☐		
	If yes, provide additional information:				

[†] The definition of "persons with political influence" is provided in point 25 of part 1 of Article 3 of the RA Law on Combating Money Laundering and Terrorism Financing.



	First Name, Last Name	Citizenship	Date of Birth	Passport Series, Number	Position

DECLARATION REGARDING AFFILIATIONS [‡]					
13.	Are there any persons affiliated with any employee(s) of the Central Bank of Armenia among the owners or the executive body of the organization?		Yes ☐ No ☐		
	If yes, provide additional information:				
	First Name, Last Name	Citizenship	Date of Birth	Passport Series, Number	Position

DECLARATION REGARDING ACTUAL BENEFICIARIES	
14	1. I, _____, as the _____ of _____ (first name, father's name, last name) _____ (status) _____, declare that the actual beneficiary of the mentioned legal entity is: (name of organization) _____ : (first name, last name) a) _____ c) _____ _____ (date of birth) (citizenship)

[‡] Family members and persons closely related to them are considered “affiliated persons.” “Family members” are blood relatives, spouses, or persons cohabitating in civil marriage. “Closely related” persons are persons who have social or professional ties with the person in question (e.g. friend, colleague, etc.).



	b) _____ (passport series/number)
	2. The person listed in part 1 of the declaration is the actual beneficiary on the following basis/bases: ☐ the person is in fact acting on behalf of or for the benefit of the legal entity, or ☐ the person exercises actual (real) control over business relations between the legal entity and the Central Bank, or ☐ the person owns 20 or more percent of the voting shares (stakes) of the given legal entity or has a privileged opportunity to predetermine the legal entity's decisions by virtue of the person's participation or a contract executed with the legal entity, or is a member of the management and/or governing body of the legal entity, or acts in concordance with the legal entity based on common economic interests. ☐ Is there any affiliation between the actual beneficiary and any employee of the Central Bank of Armenia?

QUESTIONNAIRE ON THE ORGANIZATION'S PROCEDURES FOR COMPLIANCE WITH INTERNATIONAL SANCTIONS

	Does the organization have a compliance practice?	Yes ☐ No ☐
	If yes, please provide contact information:	
1.	First Name, Last Name Position Tel. E-mail	
2	Does the organization have procedures aimed at complying with the requirements set forth in AML/CFT-related international sanctions lists?	Yes ☐ No ☐
3	Which international AML/CFT lists are used by the organization?	
4	How are compliance checks performed with regard to the lists mentioned in point 3 of this questionnaire?	Automatically ☐ Not automatically ☐
5	Does the organization, including branches or representative offices and subsidiaries, operate in	



	countries considered high-risk from the point of view of ML/TF? [§]	
6	Has the organization had a business relationship with any individual or legal entity included in AML/CFT-related international sanctions lists?	Yes ☐ No ☐
	If yes, please provide detailed information on the nature of the business relationship, including the profits received and the types of transactions.	

I certify that the information provided in this declaration is true and correct.

First Name and Last Name:	
Signature:	
Signing Date:	

[§] The list of high-risk countries published by the FATF should be reviewed for a determination of which countries are considered high-risk in this sphere.



Note: All italicized text in blue colour is for use in preparing this form and shall be deleted from the final product.

FINANCIAL PROPOSAL

Having examined the Tender Invitation with Reference Number CBA-2026-001, [Name of Bidder] offers to fulfill the contract at the total prices noted below.

[The Financial Proposal shall include the total cost of project implementation, as well as the expected post-implementation expenses over a five-year period, including but not limited to the costs of software and software licenses, ongoing support and maintenance costs, and any other necessary expenses required by the Terms of reference, comprising the combined totals of Appendix 3.1 and Appendix 3.2.]

The Armenian resident submits the financial proposal in AMD in accordance with point 4.2 of this Invitation.

Non-resident participants of the Republic of Armenia shall be expressed in United States Dollar or Euro. In such case, for Proposal evaluation and comparison purposes all prices expressed in foreign currency will be converted into Armenian Dram (AMD). The conversion shall be conducted by the Purchaser, with the exchange rate announced at its official website “www.cba.am” by the Purchaser on the date of opening of Proposals. Moreover, a contract with a non-resident participant of the Republic of Armenia can be signed in US dollars or Euro. In case of signing a contract with a non-resident participant of the Republic of Armenia, profit tax shall arise at the rate of twenty (20) percent of the contract price, payable by the Purchaser. The profit tax rate may be changed under a relevant Treaty for the Avoidance of Double Taxation between the countries of the Purchaser and the Bidder, in which case the successful Bidder shall provide the Purchaser with a Certificate of Residency, issued by the Tax Authority of its country, within ten (10) days of contract signature. If the supplier is subject to profit tax, the comparison of price proposals shall be carried out based on the total value including the profit tax.]



Lot	Purchase Item	Price AMD, EUR or USD <i>(In words and numbers)</i>	VAT AMD, EUR or USD (if applicable) <i>(In words and numbers)</i>	Total Price AMD, EUR or USD <i>(In words and numbers)</i>
1	2	3	4	5=3+4
1		{in numbers}	{in numbers}	{in numbers}
		{in words}	{in words}	{in words}

Name of Bidder (position, first name and last name)

Signature and Stamp



OPTIONAL PROPOSAL

[Here to be provided pricing for requirements marked “Desirable”]

Lot	Purchase Item	Price AMD, EUR or USD <i>(In words and numbers)</i>	VAT AMD, EUR or USD (if applicable) <i>(In words and numbers)</i>	Total Price AMD, EUR or USD <i>(In words and numbers)</i>
1	2	3	4	5=3+4
1.				
2.				
3.				
....				

Pricing for requirements “Desirable”. Such pricing may be considered for future contracting, depending on budget and need.



Note: All italicized text in blue colour is for use in preparing this form and shall be deleted from the final product.

BREAKDOWN OF FINANCIAL PROPOSAL

(Cost Breakdown Table for System Implementation, Including 1-Year Warranty Support)

The Participant shall submit a detailed breakdown of the System supply and implementation costs, clearly specifying the unit and total prices for each proposed component, including terms, schedule, and procedure for payment.

Component Number	Name	Brief description	Unit of Measurement	Quantity	Unit Price, Including VAT (If applicable) /AMD, EUR or USD/	Total Price Including VAT (If applicable) /AMD, EUR or USD/
1	2		3	4	5	6 =4x5
1.						
2.						
...						
...						

Detailed warranty service terms _____

Payment Terms _____



[In the event that an advance payment is required, up to 25% (twenty-five percent) of the total implementation cost (Contract Price) may be paid as an advance payment.]

Payment Conditions _____

Name of Bidder (position, first name and last name)

Signature and Stamp



BREAKDOWN OF FINANCIAL PROPOSAL

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.

No	Name	The annual price of the service period per year					Total Prices AMD, EUR or USD
		Year 1	Year 2	Year 3	Year 4	Year 5	
1							
2							
3							
4							
Annual Subtotals:							
VAT (if applicable) /AMD, EUR, USD/							
Cumulative total cost of expected expenses							

Terms, schedule, and method of payment _____

Detailed terms of post-warranty service _____

Name of Bidder (position, first name and last name)

Signature and Stamp



COMPREHENSIVE DESCRIPTION of Proposed Product

Name of Bidder presents below a comprehensive description of the Service proposed by bidder within the framework of the Tender with Reference Number CBA-2026-001, broken down by component.

[The participant must provide a detailed description of all the information required by the Technical Specification in their technical proposal:]

--

In addition to Appendices 4, the bidder shall submit a completed detailed response form in XLS.



CBA-2026-001_Requ
irements.xlsx



INFORMATION

About the participant's "Professional experience"

[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).]

Nº	Name of Partner Organization	Subject of Contract / Brief Description	Starting and Ending Month/Year	Dedicated team/team size in the whole Project	Bidder's role in the whole Project	Approximate value of the contract /AMD or USD/	Contacts of the Partner Organization
1.							Contact person: Position: Address: Email: Telephone:
2.							Contact person: Position: Address: Email: Telephone:
3.							Contact person: Position: Address: Email: Telephone:

** 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.



INFORMATION

About the participant's "Team members"

[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.:]

Key Personnel						
Nr.	Name	Role/Position	Main functions	Educational Background	Total Experience (in Years)	Number of years with the Current Organization
1						
2						
3						

** 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).*



Key Personnel Details

Position		Candidate ☐ Prime ☐ Alternate	
Personnel information	Name		Date of birth
	Educational Background, Professional qualifications, Training / Certification including institutions, specialization areas etc.		
	Degree/Certificates etc.	Year of Award	University/other
Present employment	Name of Employer		
	Address of Employer		
	Telephone, E-mail		
	Years with present Employer		

Summarize professional experience over the last five - ten years, in reverse chronological order.

From	To	Company / Project / Position / Relevant technical and management experience