ՀԱՅՏԱՐԱՐՈՒԹՅՈՒՆ

բաց մրցույթ կազմակերպելու վերաբերյալ

Հայտարարության սույն տեքստը հաստատված է ՀՀ ԿԲ մրցութային հանձնաժողովի 2025թ.-ի նոյեմբերի 27-ի թիվ 47 արձանագրությամբ

Հայաստանի Հանրապետության կենտրոնական բանկը հայտարարում է բաց մրցույթ, որի պայմանները ներկայացված են կից Հրավերում:

Հրապարակման ամսաթիվ՝	**09.12.2025թ.**
Պատվիրատու՝	**ՀՀ կենտրոնական բանկ** Վազգեն Սարգսյան փ. 6, ք. Երևան, 0010, Հայաստան
Ընթացակարգի ծածկագիրը՝	**CBA-2025-062**
Ընթացակարգի նպատակը՝	**Ֆինանսական հաղորդագրությունների փոխանակման ծառայության ձեռքբերում (բաղկացած երկու համակարգերից՝ Financial Message Exchange System և Central Bank Gateway System)**
Հրապարակման վայրը/Տեղեկագիր՝	**https://www.cba.am/am/SitePages/tenders.aspx**
Հայտերի ընդունման վերջնաժամկետը՝	մինչև **2026թ.-ի հունվարի 29-ը ժամը՝ 16:00-ն (GMT+4)**
Հայտերի ներկայացման եղանակը՝	Էլեկտրոնային, ուղարկել CBA-2025-062@cba.am էլ. հասցեին
Հրավերի պարզաբանման հարցման վերջնաժամկետ՝	**մինչև 2026թ.-ի հունվարի 21-ը, ժամը՝ 16:00-ը (GMT+4)**
Հայտերի բացման նիստ՝	**2026թ.-ի հունվարի 29, ժամը՝ 16:00 (GMT+4)**
Հայտերի ամփոփման նիստ՝	**2026թ.-ի մարտի 26, ժամը՝ 16:00 (GMT+4)**
Մրցույթի կազմակերպիչ՝	ՀՀ Կենտրոնական բանկ, Գնումների համակարգման ծառայություն
Հաղորդակցման եղանակ՝	**Միայն գրավոր, էլ. փոստ.** E-mail to: siran.yeganyan@cba.am cc: procurement@cba.am

Սույն ընթացակարգի արդյունքում ընտրված մասնակցին կամ մասնակիցներին կառաջարկվի կնքել ֆինանսական հաղորդագրությունների փոխանակման համակարգի կամ համակարգերի (Financial Message Exchange System և Central Bank Gateway System) մատակարարման և ներդրման պայմանագիր, ինչպես նաև՝ ներդրումից հետո սպասարկման և այլ առնչվող ծառայությունների համար պայմանագիր:

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's Protocol No. 47 dated 27th of November, 2025.

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

Issued on:	**09.12.2025թ.**
Procuring entity:	**Central Bank of Armenia** 6 Vazgen Sargsyan St., Yerevan, 0010, Armenia
Procedure Reference Number:	**CBA-2025-062**
Purpose of Procedure:	**Acquisition of a Messaging Service consisting of two interoperable systems: Financial Message Exchange System, and Central Bank Gateway System.**
Publication place:	**https://www.cba.am/en/SitePages/tenders.aspx**
Deadline for Submission of Proposals:	**Thursday, the 29th of January, 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-2025-062@cba.am**
Deadline for Requests for Clarifications of the Invitation:	**Wednesday, the 21th of January, 2026, not later than 4:00 p.m. (GMT+4)**
Date of Opening of Proposals:	**Thursday, the 29th of January, 2026, 4:00 p.m. (GMT+4)**
Notification of Award:	**Thursday, the 26th 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:** Attention to: Ms. Siran Yeganyan, Head of Procuremer Coordination Service, Central Bank of the Republic of Armenia E-mail to: **siran.yeganyan@cba.am** cc: **procurement@cba.am**

The Bidder(s) selected through this procedure will be offered a contract for the supply and implementation of one, or both systems of the Messaging Service (Financial Message Exchange System, and Central Bank Gateway System) and a contract for post-implementation support and related services.

ՀՀ կենտրոնական բանկ

INVITATION TO AN OPEN TENDER

Request for Proposals

FOR ACQUISITION OF MESSAGING SERVICE FOR THE NEEDS OF THE CENTRAL BANK OF THE REPUBLIC OF ARMENIA

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ
ԿԵՆՏՐՈՆԱԿԱՆ ԲԱՆԿ
Վազգեն Սարգսյան փող., 6, Հայաստան, 0010,
Երևան
Հեռ.՝ +374 10 592 592, www.cba.am

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.....7
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.....14
8. CONTRACT PERFORMANCE AND ADVANCE PAYMENT SECURITIES,.....15
9. EXECUTION OF THE CONTRACT.....17
10. DECLARING THE PROCEDURE INVALID.....18
11. BIDDERS' APPEAL RIGHTS.....18

Appendix 1.....19
Appendix 2.....101
Appendix 2.1.....104
Appendix 3.....109
Appendix 3.1.....110
Appendix 3.2.....111
Appendix 4.....113
Appendix 5.....115
Appendix 6.....116

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-2025-062.

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

Within the scope of this procedure, payments for subscription licenses and technical support services for the subsequent years shall be organized in accordance with the requirements of Article 15 part 6 of the Law of the Republic of Armenia "On Procurement".

The execution of payments for services in each subsequent fiscal year, as stipulated in the Contract, shall be subject to 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 bid that does not comply with the Invitation.

All matters related to this procedure shall be governed by the laws of the Republic of Armenia. Any disputes arising in connection with 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 procurement is the implementation of a Messaging Service for the needs of the Central Bank of the Republic of Armenia. The service will include a Financial Message Exchange system, and a Central Bank Gateway System, to enable secure financial message exchange, ISO 20022 compliance, centralized workflow management, and future interoperability with SWIFT and regional solutions.

The purpose of this Request for Proposal (RFP) is to invite qualified solution providers to submit comprehensive proposals for the modernization of the national financial market infrastructure. This modernization will include the implementation of the new Messaging Service.

Through this RFP, the Central Bank of Armenia seeks to engage experienced, capable, and innovative firms with proven expertise in delivering financial infrastructure projects, particularly in ISO 20022-based messaging, and secure, scalable architectures designed for mission-critical environments.

1.2. In accordance with this procedure, the procurement shall be carried out in a total of 2 (two) Lots. This RFP covers the acquisition, implementation and support of a Financial Message Exchange System, composed of Messaging Hub component - Lot 1, and a Central Bank Gateway System, composed of Gateway, Orchestration and Formatting components - Lot 2.

1.3. The Terms of Reference (ToR), attached as 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 shall 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 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 the 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 on this ground.

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 participate in the procurement process, or failure to pay the prepayment, contract performance security, and/or qualification security amount within the period specified in the invitation or contract;

  or

- refused to execute a contract as the 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), or in other duly justified cases specified in this Invitation, where the bidder's financial standing, reputation, or prior performance is deemed to adequately ensure the fulfillment of contractual obligations.

2.6. Bidders can participate in this Procedure as joint ventures (consortium or JV). 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:

- The bidder must have a minimum of 3 (three) years of proven experience in the design and implementation of financial messaging solutions for central banks, national payment infrastructures, or financial institutions.
- The bidder must have successfully completed at least three contracts of a similar nature and scope within the last 10 years. The bidder must have at least one existing support & maintenance contract.

2.7.2. The bidders failing to meet the minimum qualification requirement will be disqualified.

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 submit proposals for each Lot individually, as well as for both Lots.

3.3. Bidders may not submit more than one Proposal for the same procedure, except when submitting amendments to the Proposal provided for in clauses 3.10 and 5.7 of this Invitation.

3.4. Proposals must be submitted to the Committee no later than the Proposal submission deadline indicated in the announcement of this Procedure.

3.5. Proposals must be submitted electronically to **CBA-2025-062@cba.am**.

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

3.6. Proposals must be submitted in English.

3.7. When submitting a Proposal electronically, the following rules must be observed:

- The Reference Number "CBA-2025-062" 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 3.11 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 confirmation email will be sent to the bidder upon receipt of the Proposal.

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

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

3.10. 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 3.5, following the procedure set out in this Chapter, 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**.

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

1) An **application-statement** approved by the bidder in accordance with Appendix 2 to this Invitation, including:

   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) **The Financial Stability Report** – including financial statements for the past three (3) years (2022, 2023, and 2024) and interim financial reports for 2025. Please refer to Financial Stability requirement in Chapter 10.4 of the ToR for more details,
9) 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.
10) 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 Bidders of the Republic of Armenia shall be expressed in United States Dollars or Euros. In such case, for Proposal evaluation and comparison purposes all prices expressed in foreign currency will be converted into Armenian Drams (AMD). The conversion shall be conducted by the Purchaser, with the exchange rate announced at its official website "**www.cba.am**" 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 value 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**, the **technical proposal**, and the **bidder's overall impression**, which together carry a total weight of **70%** (60 pp for the technical proposal and qualification criteria, 10 pp for the **bidder's overall** impression). 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. Non-financial evaluation criteria are derived from the requirements set out in Appendix 1 (Terms of Reference). The detailed scoring sub-criteria, as provided in the Excel evaluation sheets, are structured to ensure traceability between ToR requirements and evaluation elements.

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. Note, that if the bidder receives less than 30% in any criterion (listed in the tables below), they will not qualify for the further evaluation.

The tables below show the breakdown of evaluation criteria for the Financial Message Exchange System and the Central Bank Gateway System.

Lot 1: Financial Message Exchange System

Evaluation Criteria - Summary of Evaluation Focus	Maximum Score
Bidder's qualification requirements – Proven experience, credibility, and long-term reliability in implementing messaging and payment infrastructure solutions for central banks and financial institutions.	15
Functional requirements - Functional coverage, interoperability, and integration capabilities.	30
Non-Functional requirements - Reliability, performance, and system availability under high-load conditions.	10

Evaluation Criteria - Summary of Evaluation Focus	Maximum Score
Technology & Architecture requirements - Scalability, flexibility, and technical robustness across hybrid and virtualized environments.	15
Security requirements - Cybersecurity governance, access control, compliance with standards, and operational resilience.	15
Implementation approach - Quality and realism of the implementation plan, governance, testing, and risk management.	15
Total Technical Score	**100**

Lot 2: Central Bank Gateway System

Evaluation Criteria - Summary of Evaluation Focus	Maximum Score
Bidder's qualification requirements - Proven experience, credibility, and long-term reliability in implementing Messaging Gateway or payment infrastructure solutions for central banks and financial institutions.	15
Functional requirements - Secure, reliable, and real-time financial message exchange supporting ISO 20022 MX and legacy HT standards, with validation, translation, routing, and monitoring capabilities.	30
Non-Functional requirements - Performance stability, high throughput, low latency, and high availability through clustering, fault tolerance, and disaster recovery.	10
Technology & Architecture requirements - Scalable, resilient, and flexible architecture supporting hybrid or cloud deployment, system compatibility, extensibility, and load balancing.	15
Security requirements - Comprehensive cybersecurity governance with encryption, access control, monitoring, and compliance ensuring secure and auditable operations.	15
Implementation approach - Clear implementation roadmap, realistic timelines, defined milestones, risk mitigation, and readiness for reliable deployment.	15
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 is the offered price 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.

6.11. "Bidder's overall impression" is the overall impression of the bidder based on reference checks, site visits, and interactions during the evaluation process. It reflects CBA's confidence in the bidder's professionalism, transparency, responsiveness, implementation experience, and ability to act as a reliable long-term partner.

6.12. 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.

6.13. 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.

6.14. 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.

6.15. 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.

6.16. 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.

6.17. 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.

6.18. 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.

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

6.20. 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.

6.21. 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.

6.22. 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 where applicable under this Invitation. 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, shall be submitted as a scanned copy of the original guarantee or confirmed through an authenticated SWIFT message, provided that the bidder submits the original document to the Purchaser, upon request, no later than upon agreed deadline.

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.

<u>It is essential to provide confirmation through an authenticated SWIFT message, which is the standard method for verifying the issuance of a guarantee.</u>

The Purchaser may give its consent to release the Guarantor Bank from obligations upon receipt of the authenticated SWIFT confirming the issue of the Guarantee. Banks may arrange the exchange of these messages through third correspondent banks. All associated costs related to the issuance, transmission, and confirmation of the guarantee, including any intermediary bank fees, shall be borne by the bidder.

In the case of bid security provided in the form of a bank guarantee, the Purchaser shall notify the issuing bank in writing 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.

7.6. The Purchaser shall submit the request for payment to the bank that issued the guarantee in writing within 5 (five) working days following the date on which the basis for the payment of the guarantee arises.

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, 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, taking into account the bidder's credit rating, or in other duly justified cases - financial standing, reputation, and prior performance, to ensure adequate fulfillment of contractual obligations. 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 final date of full performance of the contractual obligations under the implementation period, and thereafter for the warranty phase.

- In the case of a bank guarantee, the contract security shall be submitted in a format approved by the Purchaser prior to contract signature. Non-resident bidders must provide confirmation through an authenticated SWIFT message, which is the standard method for verifying the issuance of a guarantee. The Purchaser may consent to release the Guarantor Bank from its obligations upon receipt of the authenticated SWIFT confirmation. Banks may arrange the exchange of these messages through third correspondent banks. 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 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 The Purchaser shall submit a written request for payment of the contract performance security to the bank within 5 (five) working days following the date on which the basis for

payment arises. 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 make the written notifications regarding the return of a contract performance security as follows:

- in the case of a bank guarantee, to the issuing bank, within 5 (five) working days following the date on which the basis for return arises,
- in the case of a penalty, 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 full performance of the contractual obligations.

8.8 The Purchaser shall notify the issuing bank in writing regarding the return of the advance payment security within 5 (five) working days following the date on which the grounds for its return arise. The procedure for repayment of the advance payment shall be defined in the contract.

8.9 All bank guarantees shall be unconditional and irrevocable issued by a bank agreed with the CBA.

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 Service 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 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 of the reasons 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 prior to the proposal submission deadline, in accordance with the procedure established by the Code.

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

Appendix 1

Tender Invitation
Reference Number: CBA-2025-062

TERMS OF REFERENCE

LOT	Name	Technical Description	Unit of Measurement	Quantity
1.	Acquisition of Financial Message Exchange System (Messaging Hub component) for the Needs of the Central Bank of the Republic of Armenia.	The technical specification is presented in detail in Terms of Reference and applies together with the General Terms & Conditions stated below	Lot	1
2.	Acquisition of Central Bank Gateway System (Gateway, Orchestration, Formatting components) for the Needs of the Central Bank of the Republic of Armenia.	The technical specification is presented in detail in Terms of Reference and applies together with the General Terms & Conditions stated below	Lot	1

Messaging Service Terms of Reference

1 Executive Summary 25
1.1 What is Being Procured 25
1.2 What is the Objective 25
1.3 Impact 26
1.4 Expected Outcome 26
2 Introduction & Project Overview 27
2.1 Purpose of this RFP 27
2.2 About Armenia Financial Sector 28
2.3 About the Central Bank 28
2.4 Overview of the Functions of the Central Bank 29
2.5 Operational Status of the Central Bank 29
2.6 Objective of the Project 30
2.7 Project Stakeholders 32
3 Scope of Work 33
3.1 Scope of Requirements 33
3.2 Adaptation to Local Regulatory, and Language Requirements 33
3.3 Multi-Year Support and Co-Development Partnerships 33
3.4 Licensing Model and Flexibility 33
3.5 Project site 34
3.6 Structured Response Template for Bidders 34
3.7 Messaging Service Components 34
3.7.1 Conceptual View 34
3.7.2 Business Capabilities 34
3.7.3 Logical View 36
3.7.4 Multi-Infrastructure Support 37
3.8 Valid responses to this RFP 38
4 Functional & Operational Requirements 39
4.1 Requirements applicable to ALL components 39
4.2 Requirements for Messaging Hub component 41
4.2.1 Message Standards 41

4.2.2 Messaging Communication 42
4.2.3 Interoperability & Integration 43
4.2.4 Operational Capabilities 43
4.3 Requirements for the Gateway component 45
4.3.1 Messaging Communication 45
4.3.2 Interoperability & Integration 47
4.3.3 Operational Capabilities 47
4.4 Requirements for component Orchestration 48
4.4.1 Orchestration and Routing 48
4.5 Requirements for component Formatting 49
4.5.1 Message Standards 49
4.5.2 Message Translation & Mapping 50
4.5.3 Message Format Coverage 50
4.5.4 Message Validation Rules Engine 52
4.5.5 Message Format Translation/Transformation 53
5 Integration Requirements 55
6 Non-Functional Requirements 56
6.1 Performance & Reliability 56
6.2 Resilience & Availability 57
7 Technology & Architecture Requirements 59
7.1 Requirements applicable to ALL components 59
7.1.1 Hardware Layer 59
7.1.2 Infrastructure Layer 60
7.1.3 Platform Layer 60
7.1.4 Application Layer 61
7.2 Requirements for Messaging Hub component 61
7.3 Requirements for Gateway component 63
7.4 Requirements for Formatting component 64
7.5 Requirements for Orchestration component 65
8 Security Requirements 66

8.1 Operational Security 66
8.2 Cybersecurity & Resilience 68
9 Synergies 71
9.1 Integrated Implementation 71
9.1.1 Fewer Integration Points 71
9.1.2 Accelerated Timeline 71
9.2 Unified Support & SLA 72
9.2.1 Single Ticketing/Escalation 72
9.2.2 Coordinated Change/Incident Management 73
10 Qualification and Other Relevant Requirements 74
10.1 General Eligibility Criteria 74
10.2 Bidder's Qualification Criteria 74
10.3 Account Management and Project Team Qualification Requirements 75
10.4 Financial Standing 75
10.5 Financial Proposal Requirements 76
10.5.1 Cost & Licensing 76
10.5.2 Cost Efficiencies and Bundled Pricing 77
10.6 Source Code Escrow Requirements 78
11 Implementation / Delivery 80
11.1 Proposed Implementation Roadmap 80
11.2 Implementation & Support 81
12 Deliverables 83
12.1 Expected Deliverables and Planned Timelines 83
12.2 Project Documentation 83
12.3 Acceptance Criteria 86
13 Acronyms and Definitions 87
13.1Acronyms 87
13.2 Definitions 91
General Terms & Conditions (T&Cs) 93
T&Cs of Payments and delivery models 96
T&Cs of Implementation Roadmap. 98

T&Cs of Penalty Calculations. 98
T&Cs of Project management Governance 99
T&Cs of Support and Maintenance..... 100

1 Executive Summary

In light of the economic growth over recent years, the Central Bank of Armenia launched an initiative in 2024 to renew its Financial Market Infrastructure. The current infrastructure components are reaching the end of their lifecycle, and the existing messaging service solution no longer meets modern business requirements. For this reason, the CBA is seeking to replace both the infrastructure components and the RTGS system (a separate RFP will be published for the latter), while maintaining full control over the acquired solutions.

1.1 What is Being Procured

The Central Bank of Armenia (CBA) is launching the procurement of two systems of its Financial Message Exchange System and Central Bank Gateway System as part of its national payment system modernization program.

1. **Financial Message Exchange System** – the central interoperability platform enabling real-time, secure, and standards-compliant exchange of financial messages among market participants and between market participants and CBA.
2. **Central Bank Gateway System** – the Central Bank–side system responsible for securely exchanging, validating, routing messages between external and internal systems, with connectivity, orchestration and formatting capabilities.

1.2 What is the Objective

The Financial Message Exchange System and Central Bank Gateway System are strategic enablers of Armenia's financial market modernization, designed to:

- Ensure secure, resilient, and high-availability connectivity across the national payment ecosystem.
- Standardize messaging in line with ISO 20022 and international best practices.
- Support interoperability between domestic systems, financial institutions, and global networks such as SWIFT.
- Centralize orchestration and routing, enabling real-time monitoring and operational control.
- Enhance regulatory visibility, compliance, and reporting capabilities.
- Provide a scalable and extensible infrastructure that supports future services, cross-border interoperability, and regional integration.
- Strengthen cybersecurity and operational resilience.

1.3 Impact

The successful implementation of the Financial Message Exchange System and Central Bank Gateway System will:

- Enable end-to-end interoperability between financial institutions and the CBA.
- Provide centralized control of messaging flows, orchestration, and operational monitoring.
- Reduce operational risks through secure and standardized workflows.
- Improve real-time visibility, resilience, and efficiency of payment system operations.
- Strengthen Armenia's readiness for innovation, cross-border interoperability, and future integration initiatives.

1.4 Expected Outcome

Bidder responses must enable CBA to assess, validate, and compare proposed Financial Message Exchange and / or Central Bank Gateway systems, and should include:

- A clear description of the solution architecture, functionality and integration strategy.
- Detailed delivery, configuration, deployment, testing, training, and knowledge transfer plans.
- Proposals for post–go-live support and maintenance with clear SLAs, disaster recovery, and business continuity provisions.
- A transparent commercial offer including itemized costs for software, services, licenses and long-term support, and any required localization or customization.
- Mechanisms such as escrow agreements to safeguard continuity in the event of vendor discontinuation.

2 Introduction & Project Overview

2.1 Purpose of this RFP

The modernization of the national financial market infrastructure aims to implement a new Messaging Service that supports secure, efficient, and future-ready communication across the financial ecosystem. This initiative requires the adoption of advanced technologies, including ISO 20022-based messaging standards and scalable, resilient architectures suitable for mission-critical operations.

The project will involve collaboration with experienced and highly capable solution providers who possess demonstrable expertise in financial infrastructure modernization, messaging system implementation, and the delivery of secure, high-availability platforms that meet the operational and regulatory needs of the Central Bank of Armenia.

The ToR is structured to reflect the two core systems of the Messaging Service, which are:

1. Financial Message Exchange System – Interbank financial message exchange system containing a Messaging Hub component – Lot 1.
2. Central Bank Gateway System – Central Bank internal Gateway consisting of a Gateway, Orchestration, and Formatting components – Lot 2.

Bidders may submit proposals for one or both systems. The document distinguishes between:

- General requirements applicable to all components.
- Component-specific requirements applicable only to the corresponding component.

Bidders should clearly indicate which system(s) they are applying for and ensure their responses address both general requirements and the relevant component-specific requirements. This structure allows flexibility for specialized bidders to compete effectively while enabling CBA to evaluate, compare, and integrate responses across the two systems and their components. Figure 1 gives a hierarchical view scope of the ToR. Requirements are presented on component level.

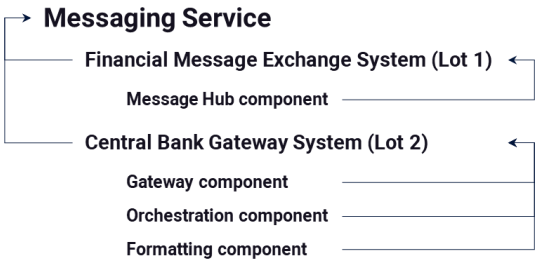


Figure 1: Hierarchical ToR scope

Note: Responses to the Central Bank Gateway System **must include** the Gateway, Orchestration and Formatting components.

2.2 About Armenia Financial Sector

As of July 2025[1], Armenia's financial system is composed primarily of 17 commercial banks, 9 insurance companies, 16 Payment Service Providers, 43 credit organizations and 23 investment companies. The banking sector continues to dominate the financial landscape, with total assets reaching AMD 11 trillion (approximately USD 28 billion), marking an annual increase of around 13%. This growth is driven by robust economic performance, digital financial service adoption, and the continued expansion of trade and services.

At the same time, total bank loans reached AMD 7.1 trillion (approximately USD 18 billion) and deposits amounted to AMD 6.7 trillion (approximately USD 17 billion) reflecting growing public trust, improved financial literacy, and enhanced digital banking outreach. The capital adequacy ratio across banks remains well above regulatory thresholds, indicating a strong and stable banking environment.

The CBA remains the primary regulator, and supervisor of the financial sector and is responsible for overseeing critical financial market infrastructures. Regulatory reforms and ongoing digital transformation initiatives such as e-wallet integration, instant payments, and modernization of banking services, have significantly improved financial inclusion. Local payment infrastructures such as Armenia Card (ArCa), which handles card and instant payment processing, plays a central role in Armenia's financial ecosystem. Alongside this, the activity of Payment Service Providers contribute to an increasingly dynamic fintech and payments landscape.

Despite ongoing regional geopolitical tensions and external economic uncertainties, Armenia has maintained macroeconomic and financial stability, supported by prudent monetary policy, resilient supervision, and an effective deposit insurance system. This has helped reinforce systemic trust and reduce financial sector vulnerabilities.

Armenia's stable, diversified, and increasingly inclusive financial system remains a core enabler of sustainable economic development, particularly as the country accelerates digitalization and regional economic integration.

2.3 About the Central Bank

The Central Bank of Armenia (CBA) is an independent public institution tasked with ensuring price and financial stability in the Republic of Armenia (RA). Established in 1993 following Armenia's independence, the CBA operates under the Law on the Central Bank and is governed by its Board, which is responsible for setting strategic direction and approving monetary and financial stability policies.

The CBA is headquartered in Yerevan and plays a central role in formulating Armenia's financial and economic policy framework. Its independence is constitutionally guaranteed, ensuring that its decisions are free from political interference and focused on long-term economic and financial stability.

In addition to its core regulatory functions, the Central Bank acts as the government's fiscal agent, managing public debt instruments and servicing state payments. The CBA also fosters innovation in the

[1] https://www.cba.am/en

financial sector, promotes financial inclusion, and drives digitization efforts across the Armenian economy. It has taken a proactive role in advancing Armenia's fintech landscape and enhancing the resiliency of national financial infrastructures.

The Central Bank actively engages with regional and international organizations, and participates in cross-border regulatory dialogues and cooperative frameworks.

2.4 Overview of the Functions of the Central Bank

The Central Bank of Armenia (CBA) has a broad and evolving mandate consistent with the principles of modern central banking. Its principal functions include:

- Monetary Policy: Formulates and implements monetary policy to maintain price stability, using tools such as interest rates and reserve requirements.
- Currency Issuance and Management: Sole issuer of the Armenian dram (AMD), responsible for ensuring adequate and secure currency supply and combating counterfeiting.
- Financial System Supervision and Regulation: Licenses and supervises banks, credit organizations, insurance firms, securities market participants, non-bank payment service providers, and investment firms.
- Payment System Oversight and Operation: Operates and oversees critical payment and settlement infrastructures, including the current RTGS system, to support safe, efficient, and reliable interbank payments.
- Government Fiscal Agent Functions: Acts as the banker and fiscal agent for the Armenian government, including management of the domestic debt market and execution of government payments.
- Reserve Management: Manages Armenia's official reserves and intervenes in the foreign exchange market when necessary to maintain market order and exchange rate stability.
- Financial Stability Monitoring and Macroprudential Policy: Conducts stress testing, systemic risk analysis, and macroprudential surveillance to pre-empt and mitigate threats to financial stability.
- Financial Innovation and Inclusion: Supports the development of digital finance, open banking, and alternative delivery channels, especially to underserved regions and populations.
- Consumer Protection and Financial Education: Promotes transparency and fairness in financial services, ensuring customer rights are protected, and leads public education initiatives on financial literacy.

2.5 Operational Status of the Central Bank

The Central Bank of Armenia operates in a stable, institutionalized, and technologically progressive environment, supported by a set of national financial infrastructures that it directly manages. Its systems are technologically mature but remain under active modernization to align with international standards. Armenia's payment infrastructure is built on a domestic (non-SWIFT) CBA interbank

proprietary network (CBANet), relying on BankMail as the secure messaging platform, Core Banking system that performs payment processing as well as general ledger functionalities, and local message format (AM-HT for interbank payment and securities transactions). Together these components provide a strong infrastructure for high-value and retail settlement.

The CBA currently:

- Operates the Electronic Payment System (EPS/RTGS), which supports real time settlement of wholesale and retail interbank payments in central bank money. However, the current solution requires enhancements to incorporate advanced capabilities such as ISO 20022 messaging, liquidity-saving mechanisms, and improved cyber-resilience.
- Oversees the Central Depository of Armenia (CDA), which is the central depository and Securities Settlement System (SSS) for non-government securities issued in Armenia and provides safekeeping, central register, clearing and settlement services to its participants.
- Acts as the central depository for RA government securities, for which it operates Government Securities Accounting and Settlement System (GSASS), that provides safekeeping, central register, clearing and settlement services to its participants.
- Supervises ancillary payment systems, including instant payments, card-based ArCa system and the STAK remittance system, in which the settlements are executed in EPS, based on multilateral net positions.

The CBA's operational strategy emphasizes automation, efficiency, and real-time capabilities across its functions. It has implemented an integrated internal accounting system and is pursuing initiatives to improve internal data analytics, cross-system interoperability, and policy decision support.

In terms of human capital and institutional capacity, the CBA employs highly qualified professionals across banking supervision, economic research, financial operations, IT, and cybersecurity. The Central Bank maintains strong international cooperation channels and draws on global expertise and benchmarks in its ongoing reform agenda.

In preparation for the modernization of the national payment system, the CBA has already undertaken a comprehensive assessment of its RTGS and Messaging infrastructures via an extensive gap assessment and requirements elicitation exercise, including looking into legal framework, business processes, and future interoperability requirements with retail, cross-border, and digital currency solutions.

2.6 Objective of the Project

The CBA is undertaking a comprehensive modernization of its national financial market infrastructure, with a focus on implementing a new messaging system. This strategic initiative aims to enhance the efficiency, security, and resilience of Armenia's financial ecosystem, while ensuring alignment with international standards and future-proofing the country's critical financial market infrastructures.

Key Components of the Project:

Messaging Service that consists of two interoperable systems:

- Financial Message Exchange System: Primary messaging hub; an application-level system for financial messaging that connects market participants to the CBA payment Infrastructure through the CBANet (CBA interbank network). The Messaging Hub is the main component of the Financial Message Exchange System.
- Central Bank Gateway System: a centralized platform within the Central Bank integrating external (Messaging Hub, SWIFT, etc.) and internal systems (Core Banking, Monetary Policy Instruments System, GSASS, RTGS etc.) to enable secure, reliable, traceable flow and transformation of financial messages ensuring unified flow management, interoperability, resilience, and extensibility. The Central Bank Gateway System consists of three main components: Gateway, Orchestration and Formatting.

Strategic Goals:

- Ensure high levels of system availability, performance, and security.
- Achieve compliance with global standards, including the BIS Principles for Financial Market Infrastructures (PFMI).
- Enable full support for ISO 20022 messaging, across relevant message types and (payment) channels.
- Enhance operational resilience, including robust business continuity, disaster recovery, and cybersecurity.
- Drive greater automation, configurability, and monitoring for the messaging environment.
- Establish a foundation for future capabilities such as high-value interbank instant payments, enhanced regulatory reporting, and regional integration.
- Improve interoperability with existing CBA systems (e.g. Core Banking), SWIFT, regional solutions, and fintech ecosystems.
- Reinforce trust, transparency, and resilience within Armenia's financial infrastructure.

Implementation Approach:

The project will be governed under a unified, structured framework encompassing all phases — from planning and development to testing and deployment. Bidders may propose solutions for one or both systems of the Messaging Service, but interoperability, seamless integration, and long-term extendibility will be key evaluation criteria, where customization of existing implementations or off-the-shelf solutions are preferred over a bespoke solution.

By undertaking this modernization, the CBA positions itself to meet growing demands in terms of transaction volumes, regulatory expectations, and cross-border interoperability[2] — ensuring the long-term stability and innovation readiness of Armenia's national Financial Market Infrastructure.

[2] cross-border interoperability refers to the support of the Swift Tracker, i.e. for cross-border payments sent through the domestic Market Infrastructure (MI) notifications are sent to the Swift Tracker.

2.7 Project Stakeholders

The success of this modernization depends on effective coordination among a diverse group of internal and external stakeholders. Bidders are expected to operate in a collaborative environment and align with the roles and responsibilities of all parties involved.

Internally, key stakeholders include senior management, the Steering Committee, and departments responsible for Payment Services, IT, Information Security and Cybersecurity, Finance, Compliance and Regulation.

Externally, the project engages commercial banks, financial institutions, the Ministry of Finance, the Central Depository of Armenia, Armenia Stock Exchange, and various technology vendors and integration partners who contribute to system implementation, testing, and interoperability.

Bidders are encouraged to consider how their proposed solutions and delivery approaches will support effective engagement across this multi-stakeholder environment. Experience managing complex, cross-functional delivery in regulated financial ecosystems will be a key evaluation factor in subsequent phases.

3 Scope of Work

3.1 Scope of Requirements

The requirements outlined in this ToR are intended to represent the minimum scope of services expected from Bidders. CBA reserves the right to request additional features, services, or enhancements that may arise while discussions, implementation, or operation.

Any such additional requirements will be subject to mutual agreement between the CBA and the selected vendor(s), including scope, timelines and associated pricing. This provision is not intended to create an open-ended obligation, but rather to ensure that the proposed solution remains adaptable to evolving needs and regulatory expectations.

If Bidders fail to address certain requirements entirely or provide responses that are incomplete or not aligned with the stated expectations, the CBA will follow up on those items, particularly on requirements deemed critical to the assessment.

3.2 Adaptation to Local Regulatory, and Language Requirements

The solution must demonstrate an ability to localize messaging, formatting and orchestration services to adapt to local regulations, reporting and language needs. Documented examples are required showing successful adaptation of business rules, validation logic, and user interfaces to meet local market practices and regulatory compliance obligations. Adherence will be evaluated based on the quality and completeness of documentation and descriptions provided by Bidders, detailing how the solution will comply with these localization requirements.

3.3 Multi-Year Support and Co-Development Partnerships

The Bidder must offer a multi-year support agreements covering a minimum of 10 years from system acceptance, including defined SLAs and performance guarantees. The proposal must demonstrate an aligned product roadmap that supports the Central Bank's long-term objectives and provide structured opportunities for co-development and joint innovation throughout the support period. The Central Bank reserves the right to negotiate additions, deletions, or modifications to the multi-year support terms and SLA submitted by Respondents.

3.4 Licensing Model and Flexibility

Bidders must explain the licensing model used for the Financial Message Exchange System and / or Central Bank Gateway System.

3.5 Project site

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

3.6 Structured Response Template for Bidders

To support a fair, consistent, and efficient evaluation process, bidders are kindly requested to structure their proposals using the response document templates provided with this RFP. The templates are intended to provide clarity on what information the CBA seeks to gather at this stage of the procurement process.

3.7 Messaging Service Components

3.7.1 Conceptual View

To seamlessly migrate Central Bank's various services to a modern, modular architecture, the new platform shall be built on pluggable services. This approach enables incremental upgrades and ensures that new services or instruments such as tokenized assets can be added at any time without major architectural changes.

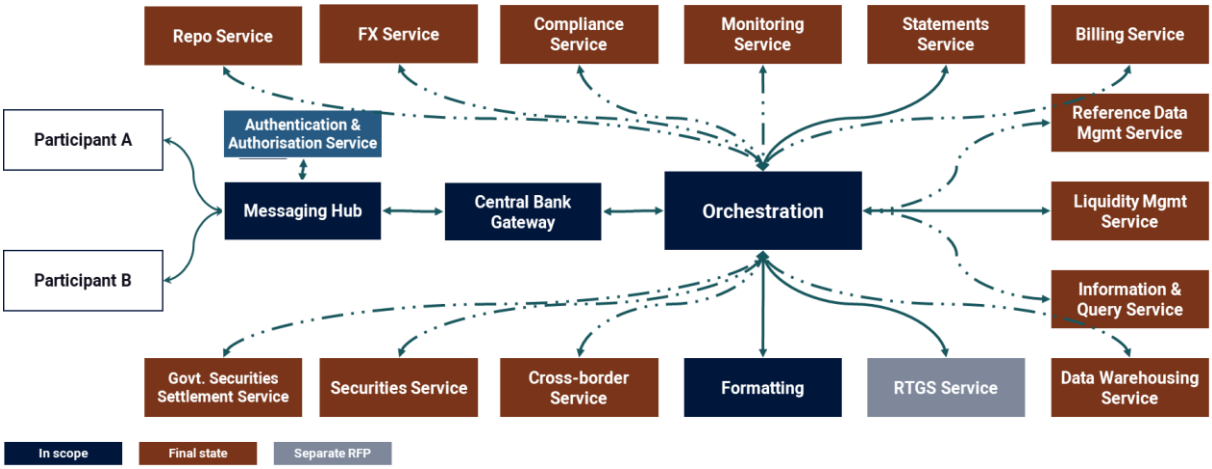


Figure 2: Conceptual view on the financial market infrastructure

Note: The scope of this ToR includes the Messaging Hub and the Central Bank Gateway, Orchestration and Formatting.

3.7.2 Business Capabilities

The **Messaging Hub** component is the platform that receives, manages and delivers messages among the participants (with CBA also acting as a participant in this context). It functions as an intermediary to simplify and streamline communication between market participants. It is essential to recognize that in

many jurisdictions, SWIFT serves as the Messaging Hub within the financial infrastructure. However, in Armenia financial messages are transported using a proprietary network and messaging platform. This solution is nearing the end of its lifecycle and requires replacement. The CBA seeks to elicit potential vendors capable of providing state-of-the-art solutions for the replacement. Its key business capabilities include:

- Grouping and managing endpoints (i.e. message queues, API endpoints, and Web endpoints) and ensuring adherence to security and connectivity policies, including participant authentication and authorisation.
- Receiving messages sent by a participant through message queues, API calls, or Web requests.
- Performing technical validation of received messages.
- Determining the appropriate recipient of the message.
- Delivering the message to the designated recipient.
- Ensuring message integrity, authenticity, and non-repudiation.
- Providing the sender of the message with at least a delivery status confirmation of the message.

The **Gateway** is the component within CBA that receives messages intended for further processing by CBA internal systems. It is operated on premises and encapsulates messaging-specific control information (non-payload) to separate it from the transaction payload data which is processed by the respective CBA business applications. Its key business capabilities include:

- Providing CBA with certificate-based access to the Financial Market Infrastructure through CBAnet and the Swift network, with the latter accessed via CBA's Swift Alliance Access/Entry instance.
- Enabling CBA to send and receive messages through predefined channels, including "message queues", "API", "Web (https)" and "File".
- Routing received messages to the orchestration component for further processing. If the Gateway component includes built-in orchestration capabilities, messages may be handled directly within the component.

The **Orchestration** component is responsible for coordinating multiple processing steps to ensure the successful execution of a message. It includes routing messages to the corresponding CBA internal systems and provides full visibility of an initiated instruction (submitted as a message) from start to finish. Its key business capabilities include:

- Performing checks on message references and detecting duplicates.
- Supporting formatting of incoming and outgoing messages (see Formatting Component). Formatting may be performed either by passing the message to a separate component or by using a built-in capability.
- Routing participant messages to the appropriate CBA internal systems based on business rules, conditional logic, context, or system availability.
- Processing and managing responses received from CBA internal systems.
- Handling errors and exceptions during message processing.

The **Formatting** component ensures that each message adheres to the format required for communication with external participants or for processing by the relevant CBA internal systems. It provides the capabilities needed for validation, conversion, and enrichment of messages to ensure successful interoperability and processing. Its key business capabilities include:

- Performing message validation.
- Converting messages to the required target format (e.g. AM-HT format to ISO 20022-AM and vice versa).
- Enriching messages to ensure successful processing by the corresponding CBA internal system as a "should-have" enhancement.
- Providing clear and detailed failure information in cases of unsuccessful validation, conversion, or enrichment.

3.7.3 Logical View

Figure 3 provides a logical view of the components that make up the platform.

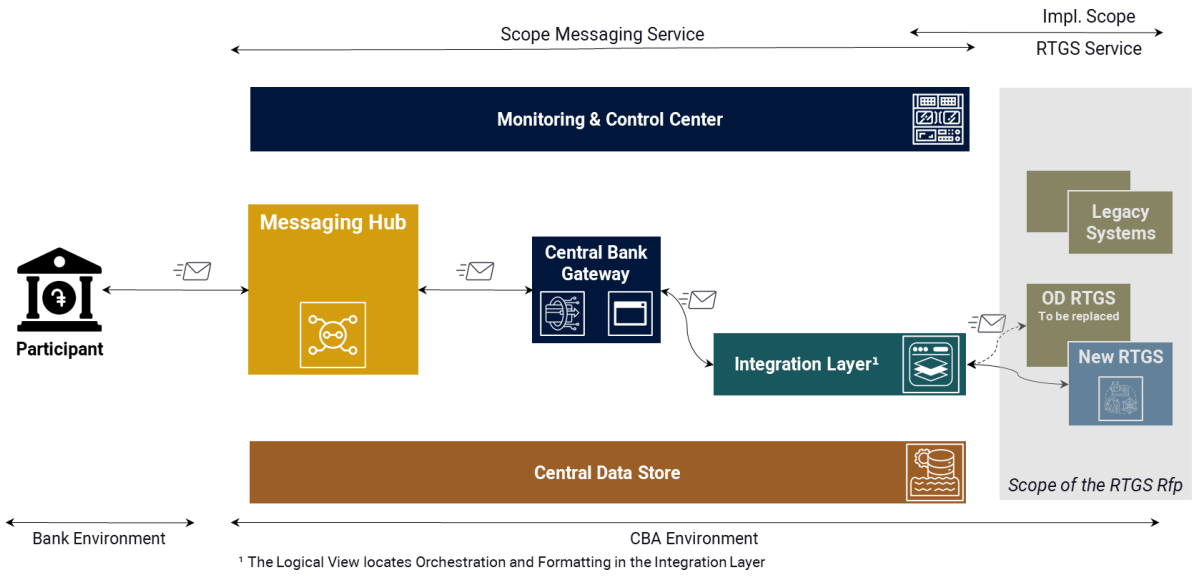


Figure 3 Logical view

At a later stage support for monitoring and control, represented as "Monitoring & Control Centre" in *Figure 3* can either be one integrated component within CBA's Market Infrastructure or through the vendor-provided plugins, as depicted in *Figure 4*. The Monitoring & Control Centre will be part of CBA's Web Portal, which will provide functionality to CBA internal staff and also to the market participants.



Figure 4 Monitoring & Control Centre on the basis of plugins

The Central Data Store will be either designed as a single consolidated data repository or implemented as an integrated environment combining multiple component-specific databases, as shown in *Figure 5*.

This flexible approach allows vendors to integrate their respective data stores into the Central Data Store while maintaining a unified data architecture.



Figure 5: Central Data Store integrating component-specific databases

For the CBA target infrastructure, it is planned to develop the Central Data Store, the Web Portal, as well as use the vendor-provided plugins for the Monitoring & Control Centre. Purpose of the information given above is to provide Bidders with the end-to-end context.

As per the current design, the Central Bank intends to provide market participants with a minimal footprint. This means that market participants will receive clear technical documentation and guidelines on how to connect and interact with the Messaging Hub.

3.7.4 Multi-Infrastructure Support

Figure 6 depicts the infrastructure the Messaging Service must support.

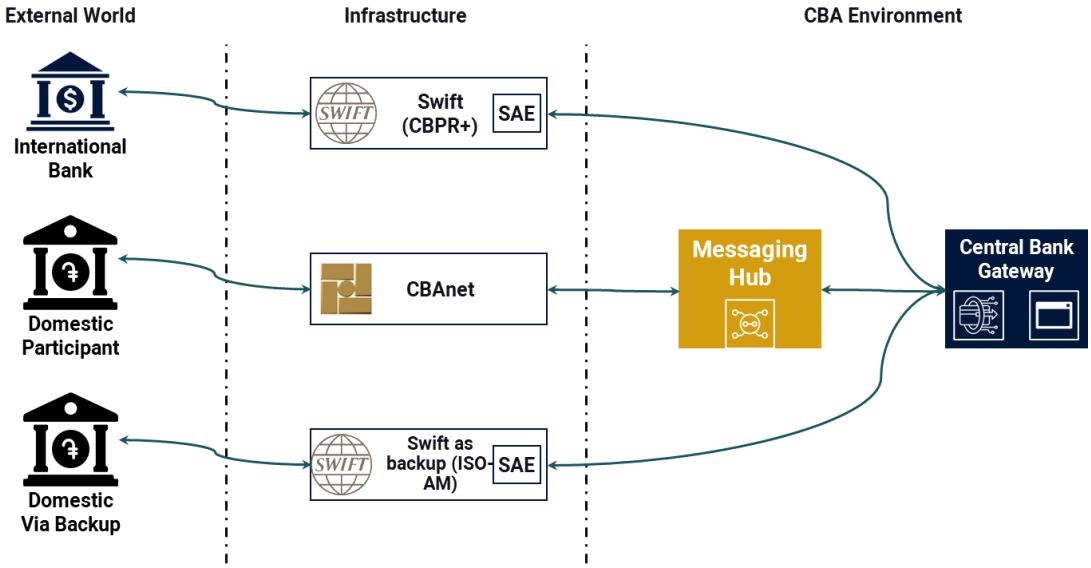


Figure 6: Infrastructures to support

The Messaging Hub (as the main component of the **Financial Message Exchange System)** is the component that enables secure and efficient message exchange between market participants, including the Central Bank. It provides multiple connectivity channels for participants to send and receive messages, ensures the secure transport of financial messages, and supports participant management, technical validation, and routing. This Messaging Hub functions as a domestic message exchange network.

The **Central Bank Gateway System** is the Central Bank's internal messaging service, responsible for managing message flows after they are delivered to the Central Bank through the Messaging Hub or other channels. Its scope includes receiving and sending messages, executing validations, performing

message formatting, enabling flow orchestration, and routing messages to the appropriate CBA internal systems.

The **distinction between these two systems** enables them to operate separately and independently, providing flexibility and resilience in the architecture.

3.8 Valid responses to this RFP

Each bidder or consortium of bidders is required to respond to this RFP by covering the scope defined in *Figure 7*. Responses that do not cover the Orchestration and / or Formatting as part of the Central Bank Gateway System are not considered valid.

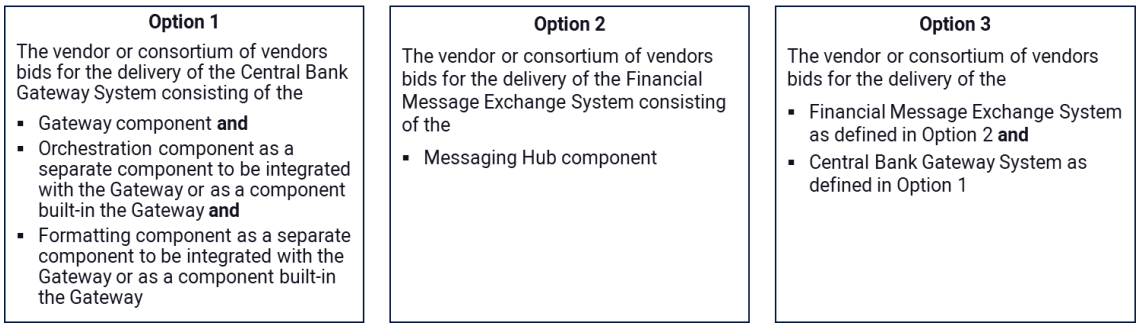


Figure 7 Valid response options

4 Functional & Operational Requirements

4.1 Requirements applicable to ALL components

Multilingual Support & Unicode Compliance

The solution shall provide multilingual user interface. Standardized coding systems and Unicode compliance must be supported to enable accurate rendering of multiple languages and character sets. Bidders must describe available language packs, font management capabilities, and any limitations in multilingual deployment or support.

End-to-End Message Lifecycle Traceability

The solution must offer full lifecycle traceability for each message, from intake to delivery, with accessible interfaces for monitoring and reprocessing. Traceability must cover message sent/received events, real-time event logging, acknowledgments, and any transformation or enrichment applied. Reprocessing must include the ability to identify and retrieve messages that failed or were delayed, inspect their full history and content, and re-initiate processing or controlled re-sending after resolving the root cause (e.g. connectivity restoration, system recovery, or corrected configuration). Access to traceability functions must be role-based. Each participant must be able to trace only their own messages, while the system operator must have the ability to trace and manage all messages across the platform. Bidders must describe tracking features and user interface capabilities, including options for search, filtering, audit logging, reprocessing, and controlled message re-sending. The solution must also provide the ability to export traceability data and events to external monitoring systems. If the solution includes a built-in monitoring system, Bidders should describe its features in addition to available export mechanisms, supported formats and protocols, and configuration options.

Timestamped Processing Logs and Retention

The solution must maintain precise, timestamped logs for all message processing events including scheduling activations/deactivations and detailed real-time processing steps. Logs must be secured, support configurable retention policies aligned to regulatory requirements. They should include automated archival of both operational logs, which record system-level events such as routing, validation, queuing, acknowledgments, failures, and recovery activities, and work logs, which record user or participant actions such as manual resubmissions, annotations, configuration changes, and administrative operations. The level and depth of logging should be configurable to balance operational visibility with performance and storage considerations. Bidders should explain logging accuracy, security, and retention settings, and compliance mechanisms.

Administrative and System Event Logging

The solution must log administrative actions. Logging must also capture configuration changes, API calls, retries, and system failures, with secure access controls. In addition, the solution must record user-related activities such as user creation and modification, role and permission delegation, changes to access rights, and user operations performed within the system. Bidders must describe audit scope, accessibility, and reporting features for administrators and auditors.

Message Storage & Traceability

The solution must maintain a centralized repository for storing all processed messages with search, filtering, and export capabilities. Operators must be able to view both sent and received messages, and export results, with all export actions securely logged and subject to role-based permissions managed by the Information Security (InfoSec) function. Filtering must support message type, participant, status, unique number, date/time. The repository must also include event logs, with the ability to view details, filter by event type, user, and time, and export. Archive management features must allow moving messages from the main archive to a deleted archive and restoring them if required. The solution must comply with data retention (e.g. 5+ years) and audit requirements, including legal archiving for a minimum number of years compliant with regulatory retention policies as defined by CBA.

User Roles and Access Model

The solution must provide a role-based access model to ensure secure and appropriate use of all system functions. The Bidder should describe the role model in detail, covering functional roles and permissions, segregation of duties, and options for user management (e.g. creation, modification). The model must support both users within the Central Bank and market participants. Bidders must explain how the proposed solution supports role definition, administration, monitoring, and compliance with security and governance requirements.

Data Accessibility and Integration Across Components

All components of the Messaging Services platform must support secure, structured data storage and provide standardized access mechanisms (e.g. database views) to enable centralized data retrieval through the Central Data Store. The Central Data Store is a logical integration layer and will not be procured as part of this RFP. Bidders are required to ensure their components can expose data in a standardized, secure, and consistent manner to enable future integration. Data must be accessible without duplication and must support reporting, monitoring, and regulatory compliance. Long-term retention and efficient retrieval must align with regulatory and operational requirements.

Web-based GUI and API Exposure

The solution must provide a dedicated web-based GUI to enable operational monitoring and administration for the Central Bank and market participants, applicable to the Financial Message Exchange System and to the Central Bank Gateway System (Gateway, Formatting, Orchestration components). The GUI must provide real-time visibility into message traffic, routing flows, and processing status; it must allow users to perform operational tasks such as message resubmission and prioritization where applicable, support free-text correspondence, annotations on individual messages, and file uploads. All functions available through the Web GUI must also be exposed via secure, documented API endpoints to enable seamless integration. The GUI must be developed using a standardized and secure architecture that supports role-based access control, extensibility for future enhancements, and callback mechanisms accessible through both the interface and the API. Bidders must describe GUI capabilities, API coverage and documentation standards, security and access control mechanisms, and provisions for extensibility and future integration.

Monitoring and Alerting
The solution must provide dashboards with real-time tracking of message states (e.g. received, validated, routed, delivered) and enable configurable alerts for delays, failures, and SLA breaches. Alerts must support customizable thresholds and multiple delivery options such as email or webhooks. Bidders must describe available monitoring features, notification channels, and alert configuration options.

4.2 Requirements for Messaging Hub component

The **Messaging Hub** component is regarded as the central component through which messages from market participants are processed. It provides certificate-based access to the Financial Market Infrastructure through CBANet and allows market participants to send and receive messages via a pre-defined set of channels / protocols. Upon receipt of the message, the Messaging Hub performs a technical validation, determines the recipient of the message, updates the message signature and delivers the message to the receiving party. Requirements are as follows:

4.2.1 Message Standards

Multi-Stack Format Handling
The solution must support processing across multiple messaging formats (e.g. the Swift MT-like standard HT exchanged via an XML envelope, ISO 20022-AM) with the ability to distinguish per participant, transaction type, or business rule. The Messaging Hub must remain format-agnostic, apart from enforcing the standardized envelope for routing and security. Routing must be based on the Application Header (DataPDU). Mapping or translation between formats is not part of the Messaging Hub and will instead be handled by the Formatting component within the Central Bank Gateway System. Bidders must describe how the system manages format coexistence and ensures consistent processing logic across all of them.

Support for ISO 20022 Messages
The Bidder's solution must support the processing of messages structured in accordance with ISO 20022 and other standardized message definitions. The focus is on supporting XSD and/or JSON schemas, including their respective validation mechanisms. The solution must provide robust technical validation using the XSD (and/or JSON) schemas to ensure structural and syntactical compliance. The solution must be extensible to support additional message categories (e.g. Securities, FX) and new schema versions in future phases, ensuring coexistence and backward compatibility. Bidders must describe schema handling, validation capabilities, version management, and how extensibility is achieved without disrupting existing message processing.

Batch File Integration
The Bidder must confirm that the proposed solution supports the ingestion and processing of batch files in formats such as CSV. Capabilities must include file validation, scheduling, secure transfer mechanisms (e.g. SFTP), and error handling suitable for production use.

4.2.2 Messaging Communication

Connectivity
The solution must provide market participants with comprehensive guideline documentation, technical libraries, and software development kits (SDKs), where applicable, to facilitate seamless connectivity through the Messaging Hub, which serves as the primary interface between participants. Connectivity will occur via the Messaging Hub, not directly to the Gateway. The solution must support multiple connectivity modes, including APIs and / or messaging queues, and must enable both application-to-application (A2A) and user-to-application (U2A) access. It must provide participant and user management capabilities with role-based access control, and ensure secure and authorized connectivity. Bidders must detail the available connectivity modes, access management, integration support, and clarify any U2A scenarios involving direct Gateway access.

SLA-Based Prioritization, Retry, and Resilience Handling
The solution must support real-time message prioritization, SLA-based delivery, automated retries, and a Store-and-Forward (S&F) mechanism to ensure resilience in distributed deployments (i.e. if the system is spread across multiple nodes or sites). Message prioritization must be applied at the transport and queue management layer of the Messaging Hub, based on envelope attributes and queue level (e.g. sender/receiver, message type) rather than detailed payment content. The S&F mechanism must guarantee reliable queuing and delivery in case of temporary connectivity or availability issues, ensuring message integrity and processing sequence upon recovery. Bidders must describe how prioritization, monitoring, retry, fallback, and failover mechanisms are implemented, as well as the configuration controls available to manage them.

Message Replay & Resubmission Capability
The solution must provide a mechanism to replay or resend queued messages for participant-to-Messaging Hub and vice versa (CBA is a participant in this scenario), via UI or API, to ensure continuity after failover, recovery, or synchronization of test and DR environments. Replay must preserve original timestamps and processing sequence. Manual resubmission must integrate with queue management functionality (received, sent, waitlist, filtered, resending queue) and provide the ability to view message content and history before resubmission. In addition, the solution must support participant-initiated messages to re-receive already delivered messages, subject to appropriate access controls and audit logging. Bidders must describe initiation, monitoring, and any functional limitations of replay and resend functionality. The solution shall also support a Store-and-Forward (S&F) mechanism to ensure that validated messages are reliably queued and delivered in the event of temporary connectivity or availability issues. Bidders must describe initiation, monitoring, participant re-receipt handling, and any functional limitations of the replay and resend functionality.

Message Structure and Authentication
The solution shall perform message validation of all inbound and outbound messages to ensure compliance with the defined XML schema and messaging standards. For all received messages, the solution shall validate authenticity, integrity, and participant authorization before accepting them for processing. Only messages that pass validation shall be forwarded. In addition, the solution shall verify

that the sending participant is authorized to send the given message type and shall perform duplicate detection to prevent reprocessing of identical messages. Where a message does not pass the validation checks, the solution shall generate and return a rejection message to the sender, including the appropriate error code(s) and description of the validation failure, unless in case the authentication failed. In this case the message and error should be escalated to and handled by the CBA CISO team in accordance with CBA's security procedures.

Authentication of Sender and Receiver
The solution must validate the authenticity of both the sender and receiver of each message. This shall include verification against trusted sources (e.g. participant registries, digital certificates, or other secure identifiers) to ensure that only authorized institutions can initiate or receive messages. The solution must also support digital signature and encryption to protect message integrity and prevent unauthorized access. In addition, the solution must allow the configuration of message routing rules based on sender, receiver, message type, time intervals, and message properties (e.g. format, size), ensuring messages are authenticated, routed, and delivered to the correct recipient in line with operational policies. Detailed technical requirements for authentication, digital signatures, and encryption are specified in Chapter 8 (Security Requirements). The Bidder must describe how authentication is implemented, maintained, and audited, and how failures are flagged for remediation.

Execution Logging and Diagnostics
The proposed solution must include detailed logging and diagnostic tools that allow users to trace transformation execution paths, identify failed mappings, and isolate root causes. The system must also support real-time alerts and integration with external monitoring systems such as SIEM or APM tools.

4.2.3 Interoperability & Integration

CBANet Messaging Integration
The solution must integrate with CBANet, the closed communication network, owned and operated by CBA. The solution must ensure transport layer security to guarantee data integrity and confidentiality during transmission. Bidders must provide a detailed description of supported communication and security protocols (e.g. TLS, encryption standards, authentication mechanisms) and explain how their solution will interface with CBANet for reliable and secure message transport. Bidders must de dependencies on network related components required for full integration.

4.2.4 Operational Capabilities

Guaranteed Message Delivery and Acknowledgment
The solution must support commit-confirm protocols and message persistence to ensure guaranteed, end-to-end delivery. Bidders must describe mechanisms for preventing data loss, duplication, as well as handling recovery and failover scenarios.

Real-Time Message Status Dashboards
The solution must provide real-time, role-based dashboards displaying message status at all stages (received, validated, routed, delivered, failed). Dashboards and monitoring views must be role-based, ensuring participants can monitor the status of their own messages in real time without visibility into

other participants' data. Bidders must describe UI accessibility, update frequency, and any visibility restrictions.

Manual Message Creation and Submission
The solution must provide the capability for authorized users to manually create and submit messages directly through the Web-based GUI. This functionality must allow users to input message data in structured fields aligned with supported message formats and validate messages before submission. Users must be able to preview message content, review validation results, and edit entries prior to final submission. The Bidder must describe how the solution supports manual message input, validation, editing, and submission workflows, including access control, auditability, error handling, and integration with the overall message lifecycle.

Message Resend on Participant Request
The solution must provide the capability to manually resend previously delivered messages in cases where a market participant confirms loss or non-receipt of the original message. Authorized Central Bank users must be able to locate the original message in the system, verify its status, and trigger a resend to the requesting participant. The solution must ensure that the resent message preserves the original content, timestamps, and identifiers while maintaining a complete audit trail of the resend event. The Bidder must describe how the solution supports message retrieval, verification, resend initiation, audit logging, and related security controls.

Real-Time Monitoring and Customizable Alerts
The solution must provide dashboards and real-time tracking of message states (e.g. received, validated, routed, delivered) and support configurable alerts for delays, failures, and breaches of processing SLAs with participants. Alerts must allow customizable thresholds and multiple delivery options (e.g. email, webhooks). Bidders must describe alert configuration, supported notification channels, and monitoring capabilities.

Historical Reporting and Queryable Logs
The solution must provide historical reporting with queryable logs, charts, and performance trends for message volumes, error rates, and SLAs. This includes detailed statistics such as counts of received and processed messages, and database intake, with configurable filters and support for archiving, unarchiving, restoring, and extracting logs as needed. The solution must allow users to control and define the time for retrieving and analysing historical message data, as well as generate and customize their own reports. Bidders must describe metrics coverage, visualization tools, and reporting frequency, retention and archival management features, as well as the ability to analyse resend attempts and archived work logs.

Operational Analytics
The solution must provide real-time operational analytics, including key performance indicators (e.g. throughput, retries, error rates), with configurable dashboards for monitoring system health and performance. Full analytics capabilities must be available based on granted access rights for CBA administrators. Bidders must describe the range of KPIs supported, customization options for dashboards, and how insights can be used to proactively manage operations and resolve issues.

Resource Monitoring and Bottleneck Detection
The solution must include real-time monitoring tools to detect CPU, memory, or network bottlenecks with automated alerting and resolution. Bidders must detail monitoring capabilities and remediation workflows.

4.3 Requirements for the Gateway component

The Gateway is a component of the Central Bank Gateway System (on the Central Bank-side), which receives incoming messages, performs structural, technical, and security validation, and routes the message to the target internal system of the Central Bank. The Gateway must communicate with both the Messaging Hub and external financial messaging systems such as SWIFT, as well as with CBA internal systems according to predefined protocols. While orchestration and formatting capabilities may be provided in built-in features or as separate components of the Central Bank Gateway System, this section focuses solely on the Gateway requirements. Detailed requirements for Orchestration and Formatting are described in their respective chapters. Requirements are as follows:

4.3.1 Messaging Communication

Connectivity
The solution must provide comprehensive guideline documentation, technical libraries, and software development kits (SDKs), where applicable, to facilitate seamless connectivity and interaction between the Gateway and external messaging networks such as the Messaging Hub and SWIFT as well as CBA internal systems. Connectivity between market participants (e.g. commercial banks, Treasury, and other financial institutions) and the system will occur through the Messaging Hub or SWIFT, not directly to the Gateway. The solution must provide multiple connectivity modes including APIs, messaging queues (MQ), SFTP, and Web interfaces, to ensure flexibility and interoperability. The solution must enable both application-to-application (A2A) and user-to-application (U2A) access and provide user management capabilities with role-based access control, ensuring secure, authorized connectivity. Bidders must describe supported protocols for communication with SWIFT and the Messaging Hub, as well as resources, integration support, and prerequisites necessary for establishing and maintaining connectivity.

SLA-Based Prioritization, Retry, and Resilience Handling
The solution must support message transport-layer prioritization and queue management based on predefined service level agreements (SLAs). Prioritization applies to messages residing in the Gateway's transport and internal processing queues and must be determined by attributes such as sender, receiver, receiving system, message type, SLA class. The solution must provide configurable mechanism for automated retries, fallback, and failover between nodes[3] or sites to ensure operational continuity in distributed deployments. SLA-based refers to the application of preconfigured routing and handling

[3] References to "nodes" in this context refer to the gateway nodes in a high-availability deployment, not nodes of integrated systems.

rules according to defined service levels (high-priority processing or routing to specific nodes during peak or contingency periods). Bidders must describe how prioritization is applied and monitored at the queue and transport level, how retries and fallback are triggered and managed, what configuration controls are, and how operational monitoring is performed to support resilience and SLA compliance.

Message Replay & Resubmission Capability
The solution must provide a mechanism to replay or resend processed or stored messages, via UI or API to ensure continuity after failover, recovery, or synchronization of test and disaster recovery environments. This functionality must apply to both Gateway-to-Messaging Hub/SWIFT and Gateway-to-CBA internal systems. Replay must preserve original timestamps and processing sequence to ensure message integrity and auditability. Manual resubmission must be restricted to authorized Central Bank users with appropriate access rights and must be fully integrated with queue and storage management features (e.g. received, sent, waitlist, filtered, resending queue). The solution must allow users to view message content and history before resubmission. Bidders must describe how replay and resend functionality is initiated and monitored, define user authorization and control mechanisms, and specify any functional limitations. The Solution must also support a Store-and-Forward (S&F) mechanism to guarantee a reliable queuing and delivery in the event of temporary connectivity or availability issues.

Message Structure and Authentication
The Solution shall perform message validation, including XSD schema validation and relevant cross-field checks on all messages to ensure compliance with the defined XML schema and messaging standards. For inbound communication, including messages received from the Messaging Hub/SWIFT and CBA internal systems, the solution shall validate message authenticity and integrity before further processing. Only messages that successfully pass these validation and authentication checks shall be forwarded to the relevant internal systems, or external networks. In addition, the solution shall verify that the sending system (e.g. Messaging Hub, SWIFT, or internal CBA system) is authorized to send the given message type and shall perform duplicate detection to prevent reprocessing of identical messages. If a message fails validation checks, the solution shall generate and return a rejection message to the sender, including the appropriate error codes and description of the validation failure. If the failure is related to authentication, the message and error should be escalated to and handled by the CISO team in accordance with CBA's security procedures. If the failure is related to schema or messaging standard validation, the error should also be escalated to the RTGS operational team for resolution and monitoring.

Authentication of Sender and Receiver
The solution must validate the authenticity of the sender or receiver of each message, where the sender or receiver may be the Messaging Hub, SWIFT, or CBA internal systems. Authentication shall rely on trusted sources such as BIC directories, participant registries, digital certificates, or other secure identifiers to ensure that only authorized institutions can initiate or receive messages. The Bidder must describe how authentication is implemented, maintained, and audited, including how authentication failures are flagged, escalated, and remediated. If authentication is already performed by the Messaging Hub, the Gateway should at minimum verify consistency and integrity of the authenticated message before further processing.

4.3.2 Interoperability & Integration

SWIFT Gateway Integration (Alliance Access/Entry, InterAct, FileAct)
The solution must offer native or certified integration with SWIFT gateways, including Alliance Access/Entry, InterAct, and FileAct. Bidders must describe adapter capabilities, certification or compliance status, and any dependencies on external tools required to support the integration.

SWIFT RefData Integration and Screening Services
The solution must provide full integration with SWIFT RefData services, including automated BIC validation, sanctions list screening (e.g. against relevant international or national watchlists), and GPI tracking with frequent updates. Bidders should detail integration methods, update frequency, and audit capabilities, and clarify how the Gateway interacts with external screening systems.

Standards Interoperability
The solution must natively support multiple ISO 20022 variants alongside relevant national and regional standards such as CNAPS (China), SFMS (India), SPFS (Russia). Bidders must describe the flexibility to manage coexistence across standards, and where applicable, translate or map between them to enable interoperability with external or regional systems. Bidders must also explain how the solution supports configuration for variant-specific requirements (such as message structure, field usage, or validation rules particular to each standard), and any limitations in ongoing maintenance or updates.

Open API-Based Integration and Emerging Solutions
The solution must offer an open, extensible API integration layer to enable secure and scalable integration with CBA internal systems, as well as with regional and cross-border systems, for example connectivity with neighbouring countries' payment systems or international services (e.g. SWIFT GPI). Bidders should outline API standards, scalability, governance, versioning, developer resources, and readiness to support emerging solutions and future integration scenarios.

Dynamic Multi-Network Routing
The solution must support rules-based, dynamic message routing across multiple networks, including where applicable external networks such as SWIFT or other regional and international payment infrastructures. Routing rules should be centrally managed and updated with minimal manual intervention. Bidders must outline routing logic, monitoring, and safeguards against errors.

4.3.3 Operational Capabilities

Guaranteed Message Delivery and Acknowledgment
The solution must support commit-confirm protocols and message persistence to ensure guaranteed, end-to-end delivery. Bidders must describe mechanisms for preventing data loss, duplication, as well as handling recovery and failover scenarios.

Real-Time Message Status Dashboards
The solution must provide real-time, role-based dashboards displaying message status at all stages

(received, validated, routed, delivered, failed). Administrators must have full visibility and monitoring capabilities across all messages, while participants must be restricted to monitoring the status of their own messages only. Dashboards and monitoring views must be accessible through a secure user interface, with clearly defined visibility rules based on user roles and permissions. Bidders must describe UI accessibility, update frequency, restrictions, and administrative monitoring features.

Real-Time Monitoring and Customizable Alerts
The solution must provide dashboards and real-time tracking of message states (e.g. received, validated, routed, delivered) and support configurable alerts for delays, failures, and breaches of processing SLAs. Alerts must be configurable for both administrators and, where applicable, participants, based on their respective roles and permissions. Alerts must allow customizable thresholds and multiple delivery options (e.g. email, webhooks). Bidders must describe alert configuration, supported notification channels, role-based visibility, and monitoring capabilities.

Historical Reporting and Queryable Logs
The solution must provide historical reporting with queryable logs, charts, and performance trends for message volumes, error rates, and SLAs. This includes detailed statistics such as counts of received and processed messages, and database intake, with configurable filters and support for archiving, unarchiving, restoring, and extracting logs as needed. The solution must allow users to define and control the time period for retrieving and analysing historical message data, as well as to generate and customize their own reports. Bidders must describe metrics coverage, visualization tools, reporting frequency, retention and archival management features, and the ability to analyse resend attempts and archived work logs.

Operational Analytics
The solution must provide real-time operational analytics, including key performance indicators (e.g. throughput, retries, error rates), with configurable dashboards for monitoring system health and performance. Full analytics capabilities must be available to CBA administrators, while participants shall only have access to a restricted subset relevant to their own messages. Bidders must describe the range of KPIs supported, customization options for dashboards, and how insights can be used to proactively manage operations and resolve issues.

Resource Monitoring and Bottleneck Detection
The solution must include real-time monitoring tools to detect CPU, memory, or network bottlenecks with automated alerting and resolution. Bidders must detail monitoring capabilities and remediation workflows.

4.4 Requirements for component Orchestration

4.4.1 Orchestration and Routing

Flow Orchestration is considered the core functionality of the Central Bank Gateway System, as this component is responsible for coordinating multiple processing steps, potentially involving both delivery and routing, to ensure the successful processing of a message. This means that Orchestration enables

involved parties to view the end-to-end lifecycle of an initiated instruction submitted through the Central Bank Gateway System. Requirements are as follows:

Orchestration
The solution must include a configurable orchestration engine to manage message routing, sequencing, and pre-processing, with support for business rule-driven flows, including pause/resume, parallel routing, and conditional branching based on message attributes. Bidders must explain how orchestration logic is defined, monitored, and modified without service disruption.

Dynamic Routing and SLA-Based Prioritization
The solution must support message routing based on configurable business rules, leveraging information from the Business Application Header and relevant message attributes (e.g. currency, transaction type, participant ID, receiving system). Routing logic must be easily configurable and adaptable without requiring system redeployment, ensuring adaptability to address operational changes. The solution must also support priority handling based on predefined processing rules and time sensitivity (SLA) to ensure timely delivery of critical messages. Bidders must describe routing flexibility, the criteria used to define and manage prioritization, and how routing and priority monitoring are implemented.

Multi-Network Routing & Open API
The solution must support routing across local, and global platforms through configurable business rules and secure open APIs. APIs must use standard protocols (e.g. HTTPS, SFTP, SOAP) and formats (e.g. ISO 20022, XML, JSON) to ensure seamless integration with internal Central Bank systems such as GSASS, and repo platforms, as well as with external networks. Bidders must describe supported network types, integration methods, and measures to ensure secure and efficient interoperability.

4.5 Requirements for component Formatting

The Formatting component provides the functionality required to handle different messaging guidelines and standards. Initially, the ISO20022-AM standard, the Armenian ISO guideline, and XML envelope (similar to SWIFT's XMLv2 with DataPDU) must be supported. For each supported ISO20022 standard, this service shall perform message validation based upon the corresponding usage guidelines. The service shall also provide functionality to convert messages from one standard to another. In the initial phase, only a conversion between AM-HT (HT is the Armenian Swift MT-like message standard) and ISO 20022-AM, in both directions, is required. Requirements are as follows:

4.5.1 Message Standards

ISO 20022 Message and Structured Field Support
The solution must support all key ISO 20022 (ISO 20022-AM) message types for payments and securities (e.g. pacs, camt, sese, seev) with full handling of structured fields such as remittance info,

purpose codes, and settlement details. Since the ISO 20022-AM has not yet been formally published, compliance, should be guided by the HVPS+ user guidelines. The solution must also support ISO 20022 messages in both XML and JSON formats to ensure interoperability and future readiness. Bidders must outline message coverage and any limitations in structured field support.

Multi-Stack Format Handling
The solution must support processing across multiple messaging formats (e.g. the Armenian Swift MT-like standard HT exchanged via an XML envelope, ISO 20022-AM, and other ISO variants) with the ability to dynamically switch per participant, transaction type, or business rule. The Central Bank Gateway System should remain format-agnostic, apart from enforcing the standardized envelope (e.g DataPDU) for routing and security. Message validation and mapping or translation between formats are handled within the Formatting component of the Central Bank Gateway System. Bidders must describe how the system manages format coexistence, ensures consistent processing logic across formats, and handles mapping or translation between them.

4.5.2 Message Translation & Mapping

Legacy HT Ingestion and Mapping
The Bidder must demonstrate bidirectional support for the translation of legacy format messages into ISO 20022-AM and vice versa, as well as other ISO 20022 renditions where applicable. The solution must also support wrapping HT messages into an XML envelope to enable standardized processing and routing, and unwrapping HT messages before delivery to HT-based systems. It must ensure seamless coexistence and interoperability in environments where HT and ISO 20022 (MX) formats are processed concurrently. Bidders must describe supported message types, mapping methods, coexistence strategies, and any limitations.

4.5.3 Message Format Coverage

Batch File Processing
The Bidder must confirm that the proposed solution supports the ingestion and processing of batch files containing multiple messages (e.g. CSV) allowing participants to submit several transactions within a single file. Capabilities must include file structure and content validation, message-level formatting and integrity checks, scheduling, and secure transfer mechanisms (e.g. SFTP). The solution must support unpacking the batch file into individual messages for further processing and, where applicable, forwarding validated messages to downstream systems such as the RTGS. Bidders must describe how validation, error handling, and routing of individual messages within a batch are managed.

Support for ISO 20022 and AM-HT Messages
The Bidder's solution must support all relevant ISO 20022 message types across payments, treasury, and securities domains, including but not limited to pacs.008/009, camt.052/053/054, and pain.001. In addition, the solution must support AM-HT messages, ensuring coexistence and interoperability with ISO 20022 formats. The solution must be extensible to support additional ISO 20022 message categories, such as securities, as required in future phases. It must support parsing, validation

(including XSD validation), and transformation of these messages. Bidders must provide references to live production environments where these capabilities are supported.

Support for XML Messages

The solution must support the exchange of XML-based messages beyond ISO 20022, with full validation against their corresponding XML Schema Definitions (XSDs). The solution must parse, validate, and route such messages without compromising integrity or performance. Bidders must describe the types of XML messages supported, validation methods, and how versioning and coexistence of different XML standards are managed.

Support for ISO 20022 Updates

The Bidder must provide evidence of a product roadmap aligned with ISO 20022 maintenance cycles, including timely support for future schema and rulebook updates (e.g. SWIFT-mandated changes or updates to the ISO 20022-AM usage guidelines). The Bidder must describe how clients are notified and supported during such updates.

SWIFT CBPR+ and HVPS+ Compliance

The Bidder must confirm that the proposed solution is designed to support compliance with SWIFT CBPR+ and HVPS+ standards, including readiness for future adoption of these requirements. The solution must support automated handling of version upgrades (e.g. CBPR+ v2 to v3) and compliance rule changes with minimal disruption. Bidders must describe how versioning, validation, and migration are managed to ensure continuous compliance.

Multi-Version and Namespace Support

The Bidder's solution must support concurrent processing of multiple ISO 20022 versions or namespaces (e.g. pacs.008 v08 and v09), with automated schema handling and version control to ensure operational consistency and compliance.

Version Control and Auditability

The Bidder must confirm that version control is applied to all message definitions, transformation logic, and compliance rules. The solution must include audit trails, change tracking, and rollback capabilities for all ISO 20022-related configurations.

JSON API and Hybrid Model Compatibility

The Bidder must demonstrate the ability of the solution to support real-time JSON APIs and hybrid envelope models in parallel with ISO 20022 XML messaging. The solution must enable flexible integration and message processing across formats.

Business User Mapping and Transformation Tools

The Bidder must demonstrate how the proposed solution enables business users (non-developers) to define and modify mapping and transformation logic using intuitive tools such as drag-and-drop interfaces, no-code or low-code environments. The solution should allow users to independently manage mappings without reliance on technical teams.

4.5.4 Message Validation Rules Engine

XSD Schema Validation, Versioning, and Error Classification
The Bidder must describe how the solution validates XML messages, including ISO 20022 (ISO 20022-AM), against official Schema Definitions (XSDs), supporting schema evolution, version coexistence, and backward compatibility with minimal disruption. Schema validation and related format checks shall be part of the Formatting component to avoid duplication of functionality within the Central Bank Gateway System. The solution must provide schema version control, manage dependencies, detect structural and syntactical issues, classify and report validation flagging and automated or guided remediation.

Market Practice Rule Pack Support
The solution must include built-in validation rule packs aligned with major market practices such as HVPS+. The Bidder must confirm how these rule sets are maintained, versioned, and updated.

MX Message Generation and Business Rule Validation
The Bidder must demonstrate the solution's ability to generate and validate ISO 20022 MX messages in full compliance with schema definitions and configurable message validation rules. The solution must support user-defined rules such as mandatory field checks, data type validation, and conditional logic, which must be reusable across message types, configurable without coding, and managed through a centralized interface. Business rule validation must be flexible, allowing it to be enabled or disabled during testing, migration, and production. The solution must include robust error reporting with clear, actionable feedback for remediation.

Version Control and Governance of Validation Rules
The Bidder must describe the solution's governance framework for validation and transformation rules. This must include version control, rollback capability, audit trails, and integrated approval workflows. The system must track all rule modifications and log who made or approved each change, supporting regulatory and internal governance requirements.

Real-Time and Batch Validation at Scale
The Bidder must confirm that their system supports both real-time validation on message receipt and batch-mode validation for large volumes. The solution must ensure high throughput and minimal latency under production-scale workloads, with mechanisms in place to avoid performance degradation.

Transparency of Validation Failures
The proposed solution must offer clear visibility into failed validations. The Bidder must describe how users can access detailed error logs, trace failures to specific rules or data points, and receive recommended remediation steps to resolve issues efficiently.

Structured and Unstructured Data Handling
The solution must process both structured fields and unstructured data (e.g. free-text remittance info) with configurable templates. Bidders must describe parsing accuracy, adaptability, and any limitations.

4.5.5 Message Format Translation/Transformation

Custom XML/JSON Ingestion
The Bidder must describe how the solution supports ingestion of non-standard or proprietary XML and JSON formats. The solution must include a self-service or configurable interface for defining mappings, validation rules, and transformation logic without requiring vendor intervention.

Support for Regional ISO 20022 Variants
The Bidder's solution must accommodate national or regional ISO 20022 renditions (e.g. CBPR+, SEPA, SPFS) through configurable rule sets and maintainable extensions. The Bidder must describe how such regional adaptations are implemented and maintained.

Configurable Mapping Engine
The Bidder must provide details of the solution's mapping engine, which must support transformation from multiple input formats (e.g. CSV, MT, JSON) into ISO 20022 structures. This engine must support versioning, testing, and management of reusable mapping templates.

Field-Level Enrichment and Traceability
The Bidder must demonstrate support for field-level enrichment using internal reference data (e.g. BICs, LEIs, account aliases). Enrichment rules must be user-defined, with full auditability and traceability of enriched data.

Message Enrichment, Normalization, and Auditability
The solution must support automatic enrichment of inbound and outbound messages (e.g. LEIs, UETRs) using configurable rules and external data sources (e.g. LEI registry, reference data). Enrichment must also leverage internally maintained reference tables, including supported banks, foreign exchange rates, and supported transaction types. The solution must normalize inbound messages for internal systems and convert fields as required to meet target interface specifications. Full audit traceability of enrichment and normalization processes must be ensured. Bidders must describe the flexibility of enrichment, normalization, and audit features, including how reference tables are maintained and applied.

Advanced Transformation Logic Support
The Bidder must describe how the solution supports advanced transformation logic, including nested message structures, conditional branching (e.g. if/then/else), and the creation of custom message types. These capabilities should be accessible through the user interface, without requiring custom development or professional services.

Reusable Components and Propagation Management
The Bidder must describe how the solution supports the definition and management of reusable components or logic modules (e.g. currency conversion, ID formatting) that can be shared across multiple mappings. The solution must allow centralized updates and ensure that changes propagate reliably to all dependent mappings.

Contextual Transformation and Enrichment Rules
The Bidder must demonstrate how the solution dynamically applies transformation or enrichment rules based on message context or metadata (e.g. BIC, country, transaction type). These rules must be easily maintained, tested, and deployed via the user interface, without requiring hardcoded logic.

Version Control for Mapping Templates
The proposed solution must include integrated version control for mapping templates, with capabilities to track changes, compare versions, roll back to previous versions, and apply access controls or approvals. These features must be accessible via the user interface and support audit compliance.

Execution Logging and Diagnostics
The proposed solution must include detailed logging and diagnostic tools that allow users to trace transformation execution paths, identify failed mappings, and isolate root causes. The system must also support real-time alerts and integration with external monitoring systems such as SIEM or APM tools.

5 Integration Requirements

Real-Time Integration via APIs and Message Queues
The Bidder must demonstrate how the solution supports real-time integration using APIs and message queues. The solution must handle both synchronous and asynchronous messaging patterns and ensure low-latency performance under production-scale workloads. Real-time queue interfaces must provide message history, content viewing, and counters to support operational monitoring and troubleshooting across inbound and outbound message flows.

Connector Availability for Existing Systems and Financial Message Exchange System
The Bidder must provide details on available out-of-the-box or toolkit-based connectors for integration with CBA systems (e.g. Core Banking, GSASS, RTGS) and the Messaging Hub. These connectors should be customizable and designed for upgrade-safe deployment with minimal operational disruption.

Integration with Internal Compliance and Screening Systems
The solution must support bidirectional integration with existing and future internal compliance systems, such as AML and sanctions screening, to ensure compliance checks as part of transaction processing. The Gateway shall enable ISO 20022-compliant message exchange with these systems, while the compliance and screening logic remains in the respective internal systems. Bidders must describe integration methods, supported message types, and how mismatches or alerts are reported and remediated.

Reconciliation System Integration
The solution must support bidirectional integration with reconciliation engines to ensure accurate transaction matching between internal and external systems. The Gateway shall enable ISO 20022-compliant message exchange for external reconciliation processes, including reporting of mismatches, exceptions, and remediation flows. This requirement refers to integration only, not the provision of a full reconciliation engine, which is outside the RFP scope. Bidders must describe how reconciliation messages are generated, exchanged, and audited, and how integration ensures consistency across system.

Regulatory Reporting Enablement and Schema Management
The Bidder must describe how the solution supports routing, transformation, and delivery of regulatory reports in formats such as ADF, XBRL, and ISO 20022. Mappings must be configurable given the possibility of expanding to support interoperability with other clearing and settlement schemas, and the solution must support updates to regulatory schemas with minimal disruption or manual intervention.

6 Non-Functional Requirements

The non-Functional Requirements outlined in this chapter are applicable to all four components.

6.1 Performance & Reliability

High Throughput
The solution must support high volumes of messages, including large-format and nested structures, with proven benchmark results (i.e. maximum number of messages processed per hour). The solution must support processing of at least 60,000 messages per hour, including nested and large-format structures. Performance must remain consistent regardless of message size or complexity. Bidders must provide benchmark details and describe optimization techniques and any limitations when handling complex message types.

Low Latency
The solution must ensure consistent low end-to-end message latency across all processing stages, even during peak loads. Bidders must provide benchmark data (average and peak latencies in seconds/minutes) and highlight influencing factors (e.g. message size, encryption, network), and outline optimization options.

Scalability & Orchestration
The solution must support multi-threading, vertical and horizontal scaling of containerized services under orchestration solutions, with dynamic resource allocation to match varying transaction loads. The solution must be capable of scaling to handle a 20% increase in workload within 15 minutes of demand and sustain growth to double the workload within 365 days of operation. Scaling must be coordinated across all deployed components to preserve end-to-end throughput and latency guarantees.

Monitoring & Bottleneck Detection
The solution must allow technical monitoring (system performance issues such as CPU, memory, I/O, network and throughput). It must provide real-time tracking with configurable thresholds, automated alerts, dashboards, and diagnostics, as well as integration and remediation capabilities. Monitoring must provide an integrated view across components, allowing unified tracking of message flows, latency, and failure points.

Graceful Degradation
The solution must support resilience patterns and failure isolation such as circuit breakers, bulkheads, and retry logic to maintain critical operations when under strain. Bidders must describe configuration options, fallback behaviour, and any limitations in degraded modes.

Maximum File Size Handling
The solution must support the upload, processing, and validation of large individual files up to 99MB without performance degradation or data loss. Bidders must provide benchmark results demonstrating consistent throughput and stability when handling files at or near this maximum threshold.

Performance Benchmarking Methodology
Bidder must demonstrate performance during load, stress, endurance, and failover testing based on benchmark scripts co-defined with CBA.

6.2 Resilience & Availability

SLAs & Uptime
Bidders' solution must commit to a minimum of 98% uptime (average over a 3-month period), supported by formal SLAs that cover monitoring, redundancy, incident response, and documented escalation procedures. Bidders must also outline service credits or penalties for SLA breaches.

High Availability
The solution must ensure uninterrupted operations through active clustering and seamless failover, including during planned maintenance activities, without service interruption. The solution must support a Recovery Time Objective (RTO) of less than 1 hour and a Recovery Point Objective (RPO) of less than 5 minutes. Bidders must detail backup, replication, and synchronization mechanisms to guarantee these objectives.

Disaster Recovery
The solution must support a geographically separate disaster recovery site deployment with real-time or near-real-time synchronization, automated failover, and defined RTO/RPO to ensure continuity without data loss. Bidders must describe synchronization methods, failover procedures, and testing practices to achieve high availability and resilience.

DR Testing
Bidders must provide evidence from recent DR test reports of the proposed solution, including scope, scenarios, RTO/RPO results, and outcomes, with reference to compliance standards (e.g. ISO 22301). Evidence should also note frequency, validation, and corrective actions.

Coordinated Release and Upgrade Cycles
The solution must support synchronized upgrades and configuration changes across components to ensure operational continuity and consistency of business processes. Upgrades or configuration changes must not result in partial downtime, inconsistent message states, or data loss. The solution should enable phased or rolling updates, allowing critical functions to remain online during maintenance activities.

Stress Resilience
The solution must demonstrate stability under extreme load conditions, with stress test results showing throughput, latency, resource utilization, and system behaviour under saturation. Bidders must describe testing scope, tools, frequency, and any performance limits identified.

Automated Failover & Message Rerouting

The solution must support real-time failover with automated message rerouting to alternate nodes or data centres, ensuring zero data loss and no disruption to transaction processing. Bidders must describe failover detection, switchover procedures, deployment models, and any limitations.

7 Technology & Architecture Requirements

Bidders shall submit detailed solution architecture documentation, including high-level and component-level architecture diagrams as part of their proposal. Such documentation is required to understand how the proposed solution will align with Central Bank's Financial Market Infrastructure goals.

7.1 Requirements applicable to ALL components

7.1.1 Hardware Layer

Server Infrastructure
The solution must support deployment on enterprise-grade rack-mounted, blade, and hyper-convergent servers. Bidders must specify compatibility, performance benchmarks, and recommended configurations for production-scale workloads.

Network Infrastructure
The solution must integrate seamlessly with industry-standard routers, switches, and firewalls (Cisco, Juniper, Palo Alto). Bidders must describe supported network topologies, high-availability options, and redundancy mechanisms.

Storage Systems
The platform must support SAN and NAS storage architectures with high-performance, fault-tolerant access. Bidders must provide details on supported storage protocols, scalability, and data protection mechanisms.

Backup and Recovery
The solution must integrate with enterprise backup solutions (e.g. HPE backup systems) to ensure secure, reliable data backup and restoration. Archive functions must support recovery of deleted or archived messages, including restoration from a deleted archive back to main archive. Bidders must describe supported backup strategies, archiving (when the data moves from back-ups to the archive) & retention policies, and recovery time objectives (RTO) for back-ups and retrieving/accessing archived data.

Operating System & Hardware Compatibility
The solution must support deployment on industry-standard enterprise operating systems, including Microsoft Windows Server. Bidders must specify the minimum and recommended hardware requirements (CPU, memory, storage, and network specifications) for production-scale deployments, including sizing guidelines for Messaging workloads. The response must also confirm whether the solution is certified or tested for operation on Microsoft OS environments.

7.1.2 Infrastructure Layer

Virtualization Compatibility
The solution must support enterprise virtualization platforms including VMware ESXi, Hyper-V, Nutanix. Bidders must describe resource optimization, VM management, and high-availability features.

Containerization and Orchestration
The solution must support Docker containers with orchestration by Kubernetes (K8s). Bidders must demonstrate automated deployment, scaling, self-healing, and lifecycle management capabilities.

Operating System Support
The platform must support deployment on Microsoft Windows Server and enterprise Linux distributions Bidders must specify supported OS versions, kernel requirements, and certification status.

7.1.3 Platform Layer

Relational Database Support
The solution must support enterprise RDBMS platforms including Microsoft SQL Server, and Oracle. Bidders must describe supported high-availability configurations, backup/recovery mechanisms, and database migration strategies.

Database Access for OLAP & OLTP
The solution must provide secure access to the underlying database to support both OLTP (Online Transaction Processing) and OLAP (Online Analytical Processing) capabilities. This must enable real-time monitoring, transaction statistics gathering, and analytical reporting without impacting core transactional performance. Bidders must describe supported access methods, security controls, performance isolation mechanisms, and how analytical workloads are managed alongside transactional operations.

DevOps & CI/CD Integration
The solution must integrate with CI/CD pipelines and infrastructure-as-code (IaC) tools. Bidders must describe build automation, version control, and deployment workflows.

Monitoring & Observability
The Bidder must provide details on built-in monitoring, logging tools (Zabbix, Microsoft SCOM), and alerting capabilities, including system health checks, transaction metrics, and error rate reporting. Integration with Prometheus, Grafana, or equivalent third-party tools must be supported. The solution must enable users to build custom dashboards and configure alerts for proactive monitoring and diagnostics.

Business Intelligence and Analytics
The solution must integrate with SAP BusinessObjects Business Intelligence Suite. Bidders must specify supported analytics use cases, report generation, and data source integration.

Integration and Middleware
The platform must support enterprise integration with middleware solutions. It must support common ESB architectures and integration patterns. Bidders must describe supported integration patterns, messaging protocols, and fault tolerance capabilities.

7.1.4 Application Layer

Backend Technology Support
The solution should preferably support development and deployment of applications using widely adopted backend frameworks such as .NET Core or provide equivalent capabilities that enable seamless integration with CBA's existing and future technology landscape. Bidders must describe API management and supported standards for SOAP and RESTful APIs.

Frontend Technology Support
The platform must support modern web UI frameworks (React, Angular, Vue.js, Blazor). It must also integrate with UI libraries such as Bootstrap. Bidders must describe cross-browser compatibility, responsive design, and accessibility compliance.

Deployment Flexibility
The solution must support deployment across on-premises, private cloud, and hybrid environments with seamless migration or configuration options. Bidders should specify supported models and limitations.

Extensibility
The solution must support extensibility through API gateways, plugin frameworks, and event hooks to enable custom integrations and workflows without modifying core code.

Extensibility & Customization
The solution must provide SDKs, APIs, and plugin frameworks for business logic customization, including low-code/no-code support and safe version management.

Simulation Environment
The solution must provide a non-production environment that mirrors production to validate new message types, formats, and workflows safely. Bidders must describe simulation capabilities, synchronization with production, available tools, and any functional limitations.

7.2 Requirements for Messaging Hub component

Containerization & Orchestration

The solution must support fully containerized deployments with orchestration solutions such as Kubernetes or OpenShift. Bidders must demonstrate automated lifecycle management, scaling, and upgrade orchestration capabilities.

Stateless & Scalable Architecture
The solution must use a stateless architecture that supports seamless load balancing and automatic scaling across nodes or regions, without requiring manual intervention or incurring downtime.

Horizontal Scaling & Load Balancing
The solution must provide built-in support for horizontal scaling across gateway and APIs, ensuring high availability and resilience under varying transaction loads. Load balancing mechanisms must intelligently distribute workloads across multiple service instances using orchestration solutions such as Kubernetes or OpenShift. Bidders must demonstrate automated scaling (manual and dynamic), fault tolerance, and self-healing capabilities to guarantee continuity of service during peak demand, node failures, or rolling upgrades.

High Availability & Redundancy
The solution must offer clustering, automatic failover, and geo-redundancy to maintain high availability and enable rapid recovery from node, site, or regional failures. Bidders must describe HA strategies and continuity plans.

Dual Data Centres
The solution must support deployment across dual data centres with active-active or active-passive configurations to ensure high availability, resilience, and disaster recovery. Real-time synchronization must be maintained between physically separated sites to prevent data loss and enable seamless failover in case of site-level outages. Bidders must demonstrate capabilities for transaction continuity, data consistency, and recovery time objectives aligned with financial-grade service levels.

Resource Efficiency
The solution must optimize utilization of CPU, memory, and bandwidth under varying and dynamic load conditions. It must incorporate resource management techniques to minimize overhead while maintaining performance, scalability, and reliability. Bidders must provide benchmark data demonstrating the solution's efficiency under stress scenarios, including peak transaction volumes and failover conditions.

Automated Testing Support
The solution must support automated test harnesses, mock services, and regression pipelines to validate message parsing, transformation, and routing. Bidders must demonstrate integration with CI/CD workflows to enable continuous testing, minimize manual effort, and ensure reliability during upgrades and changes.

Message Compression & Decompression
The solution shall provide built-in compression and decompression mechanisms for all inbound and outbound communications to optimize bandwidth usage and ensure efficient message exchange across connectivity layers. Bidders must specify supported compression standards, configuration options, and any limitations impacting performance or interoperability.

7.3 Requirements for Gateway component

Containerization & Orchestration

The solution must support fully containerized deployments with orchestration solutions such as Kubernetes or OpenShift. Bidders must demonstrate automated lifecycle management, scaling, and upgrade orchestration capabilities.

Stateless & Scalable Architecture

The solution must use a stateless architecture that supports seamless load balancing and automatic scaling across nodes or regions, without requiring manual intervention or incurring downtime.

Horizontal Scaling & Load Balancing

The solution must provide built-in support for horizontal scaling across gateway and APIs, ensuring high availability and resilience under varying transaction loads. Load balancing mechanisms must intelligently distribute workloads across multiple service instances using orchestration solutions such as Kubernetes or OpenShift. Bidders must demonstrate automated scaling (manual and dynamic), fault tolerance, and self-healing capabilities to guarantee continuity of service during peak demand, node failures, or rolling upgrades.

High Availability & Redundancy

The solution must offer clustering, automatic failover, and geo-redundancy to maintain high availability and enable rapid recovery from node, site, or regional failures. Bidders must describe HA strategies and continuity plans.

Dual Data Centres

The solution must support deployment across dual data centres with active-active or active-passive configurations to ensure high availability, resilience, and disaster recovery. Real-time synchronization must be maintained between physically separated sites to prevent data loss and enable seamless failover in case of site-level outages. Bidders must demonstrate capabilities for transaction continuity, data consistency, and recovery time objectives aligned with financial-grade service levels.

Resource Efficiency

The solution must optimize utilization of CPU, memory, and bandwidth under varying and dynamic load conditions. It must incorporate resource management techniques to minimize overhead while maintaining performance, scalability, and reliability. Bidders must provide benchmark data demonstrating the solution's efficiency under stress scenarios, including peak transaction volumes and failover conditions.

Automated Testing Support

The solution must support automated test harnesses, mock services, and regression pipelines to validate message parsing, transformation, and routing. Bidders must demonstrate integration with CI/CD workflows to enable continuous testing, minimize manual effort, and ensure reliability during upgrades and changes.

Message Compression & Decompression
The solution shall provide built-in compression and decompression mechanisms for all inbound and outbound communications to optimize bandwidth usage and ensure efficient message exchange across connectivity layers. Bidders must specify supported compression standards, configuration options, and any limitations impacting performance or interoperability.

7.4 Requirements for Formatting component

Scalability & Resilience
The Bidder must describe the solution's support for Kubernetes-based orchestration, including the ability to scale dynamically across pods or nodes and rapidly recover from node failures for stateless services. Expected recovery times and system behaviour under varying loads must be detailed.

Real-Time & Scalable Integration
The solution must support high-volume, low-latency communication through APIs and message queues (e.g. Kafka, RabbitMQ) for both synchronous and asynchronous processing. Bidders must demonstrate the ability to handle peak transaction loads while ensuring scalability, reliability, and backward compatibility with existing integration patterns.

Event-Driven Architecture
The solution must enable asynchronous processing using event streaming technologies, supporting guaranteed delivery, replay, and full traceability of messages. Bidders must show how the solution ensures resilience, fault isolation, and real-time responsiveness through event-driven design.

Connectors for Core Systems
The solution shall provide customizable or out-of-the-box connectors to core banking systems, messaging hubs, and integration layers. Connectors must be upgrade-safe, support industry standards, and allow configuration without extensive custom coding to accelerate deployment and reduce maintenance overhead.

Composable Architecture
The solution must use modular, reusable, and independently deployable services to enable rapid onboarding of new flows, participants, or business rules. Bidders must describe component organization, integration methods, and any limitations in flexibility or scalability.

7.5 Requirements for Orchestration component

Scalability and Resilience
The solution must support containerized deployment under Kubernetes (or equivalent), with orchestration workloads able to scale horizontally across pods/nodes. Bidders must describe how the solution ensures high availability, rapid failover, and recovery for stateless and stateful orchestration tasks, including benchmark recovery times.

Real-Time & Scalable Integration
The Orchestration Service must support real-time integration through APIs and message queues (e.g. Kafka, RabbitMQ), enabling both synchronous and asynchronous workflows. Bidders must provide evidence of peak transaction handling without degradation, including compatibility with existing integration layers.

Event-Driven Architecture
The solution must enable orchestration to be triggered by events, supporting guaranteed delivery, replay of orchestration sequences, and full transaction traceability. Bidders must demonstrate how this architecture ensures resilience, isolation of failures, and responsiveness for critical workflows.

Connectors for Core Systems
The solution must provide ready-to-use or configurable connectors to core banking systems, messaging hubs, and national payment infrastructures. Connectors must comply with industry standards, be upgrade-safe, and configurable without heavy coding to speed up integration and reduce maintenance costs.

Composable Architecture
The solution must be built on a composable architecture, with modular, reusable, and independently deployable orchestration services. This enables the rapid introduction of new workflows, rules, or participant types without reengineering the core solution.

8 Security Requirements

8.1 Operational Security

Access Control and Permissions
The solution must provide granular, role-based access control (RBAC) with dynamic permission management by user type, system role, or operational domain. All access events and permission changes must be logged with user identity, timestamp, and action details to ensure full traceability. The solution should support integration with enterprise identity and authentication mechanisms (e.g. Active Directory, SAML, OIDC) and enable multi-factor (MFA) authentication for privileged administrative accounts.

Custom Role and Duty Segregation
The solution must support the creation of custom roles in addition to predefined ones, enabling segregation of duties. It must allow flexible permission configuration to align with organizational structures and regulatory requirements.

End-to-End Encryption of Data in Transit
The solution must ensure full end-to-end encryptions for all communications and data exchanges, including APIs and administrative interfaces, using TLS 1.3 or higher (or an equivalent secure protocol). Private keys must be protected with hardware-based cryptographic modules (HSMs or tokens) and never stored in plaintext. The Bidder must describe key management processes, including generation, rotation, and revocation.

Message-Level Electronic Signature
The solution must support message-level electronic signing and verification for both inbound and outbound messages, ensuring non-repudiation and message integrity across all communication flows. The solution must support CBA approved hardware and software-based electronic signature management tools, including integration with the local HSM for signature generation and verification. The Bidder must describe how message signing and verification are implemented, managed, and audited end to end.

Encryption at Rest
The solution must implement encryption at rest for all sensitive data repositories, including databases, backups, and audit logs using strong algorithms such as AES-256 or equivalent. The Bidder must describe key lifecycle management processes, including secure generation, rotation, and destruction. Integration with centralized or hardware-based key management systems is desirable.

Certifications & Data Sovereignty
The Bidder must list all relevant cybersecurity and privacy certifications currently held (e.g. ISO/IEC 27001, SOC 2 Type II or FIPS 140-3) and confirm compliance with applicable local data protection and cybersecurity laws, including data residency or sovereignty obligations. Additional certifications or attestations (e.g. ISO/IEC 27701, GDPR alignment) are desirable.

Solution Capability (Risk Visibility and Control Management)
The solution must provide capabilities that support the organization's cyber-risk governance, including audit-ready reporting and dashboards for security events, configuration posture, and compliance status. It must support integration with enterprise GRC or risk register tools through APIs or data export, enable user activity logging and analytics for control verification, and allow alignment of policy enforcement and configuration baselines with the organization's ISMS. The solution should also provide configurable alerting thresholds and periodic compliance summaries to support management review.

Cyber Incident Response
The solution must provide technical capabilities to support incident detection, analysis, containment, and recovery, including, centralized logging and event correlation interfaces, secure APIs for integration with SIEM, SOAR, and ticketing systems, role-based access controls to isolate compromised accounts or services, and support for evidence preservation through log export and forensic data collection. The solution must offer configuration options to automate response actions such as blocking, quarantine, or service restart through standardized integrations. Support for automated threat indicators (STIX/TAXII), playbook execution, or SOAR interoperability is desirable.

Cyber Resilience and Recovery
The solution must be architected for resilience against cyberattacks, including ransomware, denial-of-service, and data corruption scenarios. It must support secure backup, replication, and restoration of critical data and configurations, ensuring integrity, authenticity, and minimal recovery time (RTO/RPO). Backups and recovery artifacts must be encrypted and protected against unauthorized modification or deletion. The solution should include mechanisms for rapid isolation or failover, such as redundant nodes, immutable storage, or snapshot rollback.

Privilege Access Management
The solution provides built-in mechanisms to control and audit privileged access to administrative interfaces, including system consoles, management APIs, configuration panels, and service accounts. It must support role-based administrative segregation between security, operations, and audit functions, and enforce least-privilege principles through granular access controls, time-limited or workflow-approved privilege elevation, and strong multi-factor authentication (MFA) for all administrative actions. Comprehensive, immutable audit logs of privileged activity must be maintained and exportable to the organization's SIEM for correlation. Integration with enterprise PAM solutions (e.g. CyberArk, BeyondTrust, Thycotic, HashiCorp Vault) must be supported via standardized protocols such as RADIUS, LDAP.

Security Monitoring and Logging
The solution must provide continuous security monitoring to detect anomalies, unauthorized access, and indicators of compromise. All security-relevant events must be logged in an immutable, tamper-resistant format and integrate with the enterprise SIEM via standard interfaces (e.g. Syslog, JSON, or API). The Bidder must configure and maintain monitoring, alerting thresholds, and event correlation rules, ensuring timely review and escalation of alerts. Support or behavioral analytics, AI-based anomaly detection, or SOAR integration is desirable.

8.2 Cybersecurity & Resilience

Governance Framework

The Bidder must demonstrate alignment with established cybersecurity and risk management frameworks such as NIST Cybersecurity Framework 2.0, ISO/IEC 27001:2022, or equivalent standards. The Bidder must maintain enterprise-level information security governance, including a documented and approved security policy, clearly defined roles and escalation paths, and a risk management methodology aligned with ISO 31000/ISO 27005 principles. Evidence of assurance activities (e.g. internal audits, certification audits, SOC 2 reports) must be provided. Continuous improvement mechanisms (e.g. KPIs, KRIs, or OKRs) are desirable to demonstrate active maturity management.

Cyber Incident Response

The Bidder must maintain a formally documented and approved Cyber Incident Response Plan (IRP) outlining procedures for detection, escalation, containment, eradication, recovery, and post-incident review. The IRP must clearly define responsibilities, communication channels, and escalation paths, including coordination with CBA's incident management process. The Bidder must provide evidence of regular vulnerability scanning, penetration testing, regular incident response exercises, and tracking of corrective actions. Reporting obligations to CBA must be met within SLAs or regulatory timeframes. Integration with CBA's IRP and incident communication workflows should be supported.

Cyber Resilience and Recovery

The Bidder must maintain and periodically test documented cyber-resilience, disaster recovery, and business continuity plans to ensure uninterrupted operations during and after security incidents. These plans must address critical services, communication procedures, and clearly defined recovery time objectives (RTOs) and recovery point objectives (RPOs) aligned with CBA's resilience expectations. The Bidder must provide evidence of regular recovery testing, including backup restoration validation, ransomware-simulation drills, and corrective action tracking. Coordination with CBA's continuity and crisis management framework must be demonstrated through defined notification and escalation procedures. Independent assessments or certifications (e.g. ISO 22301) are desirable.

Third-Party and Software Supply Chain Security

The Bidder must maintain a formal Third-Party Risk Management and Supply Chain Security Program aligned with recognized ISO/IEC or NIST. This program must include processes for supplier risk assessment and due diligence prior to onboarding, contractual cybersecurity requirements ensuring confidentiality, integrity, and availability of CBA data, ongoing supplier monitoring and annual re-assessment, third-party incident reporting obligations with defined breach-notification timelines, and subcontractor flow-down clauses to ensure equivalent security standards. The Bidder must provide evidence of vendor-risk assessments for key suppliers supporting this solution. Certification under ISO/IEC 27036 or NIST SP 800-161 is desirable. The program must include detailed and enforceable procedures for each of the listed elements.

Secure Software Development and Supply Chain Integrity

The solution must be developed and maintained in accordance with secure software development lifecycle (SSDLC) practices, incorporating security by design, code review, and dependency control. It must provide verifiable assurance of software integrity through digitally signed source code and

binaries, verified update packages (e.g. code-signing, checksum validation), and a Software Bill of Materials (SBOM) detailing all third-party and open-source components, their versions, and licensing. The solution must support automated vulnerability scanning and dependency monitoring throughput the build and deployment pipeline, as well as secure update mechanisms resistant to tampering and downgrade attacks.

Vulnerability and Patch Management
The Bidder must maintain a documented vulnerability and patch management process covering all components of the proposed solution, including operating systems, middleware, databases, and third-party libraries. The process must define clear timelines for applying patches by severity (e.g. critical within 72 hours of release) and include continuous vulnerability scanning with periodic remediation reports to CBA. Emergency patching procedures, rollback testing, and change-control approvals must be clearly defined. The solution must support secure patch deployment mechanisms such as code signing, validation, and rollback. Integration with vulnerability management platforms (e.g. Tenable, Qualys, OpenVAS) is desirable.

Privileged Access Management
The Bidder must operate and maintain a corporate privileged access management (PAM) program covering all systems and infrastructures used to deliver, host, or support the proposed solution. All privileged accounts under the Bidder's control must be managed through a secure PAM platform with credential vaulting and automatic rotation, session recording and monitoring, and dual-approval or break-glass procedures for emergency access. The Bidder must provide evidence of PAM policy enforcement, including periodic access reviews and revocation of dormant or shared credentials. All privileged sessions involving CBA data or environments must be fully auditable and attributable to individual identities.

Data Loss Prevention
The Bidder must implement and operate controls to prevent unauthorized disclosure or exfiltration of CBA data from any environment where it is hosted or processed. These controls must include DLP monitoring of data in motion, at rest, and in use; content inspection with contextual policy enforcement; encryption or tokenization of sensitive fields; and restrictions on removable media and external file transfers. The Bidder must classify and label sensitive data in alignment with CBA's data-classification policy. Integration with enterprise DLP or CASB tools for centralized visibility and control is desirable.

Secure API Management
The solution must enforce strong API-level security controls, including authentication, authorization, rate limiting, input validation, and encryption of all API traffic. APIs must be protected against injection, replay, privilege escalation, and denial-of-service attacks in line with OWASP API Security Top 10 recommendations. The Bidder must maintain documented API security practices covering key management, version control, change approval, and vulnerability testing. APIs must provide standardized audit logs for integration with SIEM/SOC systems. Support for mutual TLS, OAuth 2.0/OpenID Connect, and signed tokens (JWS/JWT) is desirable.

Business Continuity and Crisis Communication

The Bidder must maintain and periodically test Business Continuity and Crisis Communication Plans (BCP/CCP) aligned with ISO 22301 and CBA's continuity framework. These plans must define recovery time objectives (RTOs), recovery point objectives (RPOs), and fallback procedures to ensure service availability during cyber incidents or infrastructure failures. The Bidder must establish clear communication protocols with CBA for incident notification, escalation, and stakeholder coordination, including regulators and critical participants. Evidence of annual continuity exercises and follow-up corrective actions must be provided. Integration of BCP with the Bidder's incident response and disaster-recovery processes is required.

9 Synergies

Where Bidders propose both systems, additional benefits such as integration, accelerated implementation timelines, cost efficiency, and unified support will also be evaluated. This section should only be responded to by bidders applying to both Lot 1 (Financial Message Exchange System) and Lot 2 (Central Bank Gateway System). The synergy bonus shall be applicable to Lot 1 only in the event that the same Bidder is awarded Lot 2.

9.1 Integrated Implementation

9.1.1 Fewer Integration Points

Native/Pre-Built Integration
Bidders must describe the extent to which systems are natively integrated or pre-integrated and explain the mechanisms for inter-system communication (custom API, shared database, etc.). This reflects the potential benefits of reduced implementation risk, and interoperability.

Elimination of Custom Development
Bidders must specify the level of custom API development or third-party middleware required to enable integration between their systems.

End-to-End Use Cases
Bidders must provide examples of cross-functional workflows already enabled across the systems. Bidders must also describe how these services interact technically and functionally, including communication mechanisms, error propagation, and audit traceability.

Data Model Consistency / Single Integration Layer
Bidders must confirm whether their systems share a unified data model or repository and explain how this minimizes integration complexity.

9.1.2 Accelerated Timeline

Shared Implementation Team
Bidders must indicate whether the same Delivery team will deploy all selected systems and describe how this reduces handoff delays or coordination overhead. The plan must highlight key implementation phases, dependencies, and responsibilities, and must be accompanied by a resource plan describing the required role, estimated workload and involvement, and indicating which resources are already available and which would need to be additionally hired.

Phased vs Parallel Rollouts
Bidders must outline whether their deployment approach supports parallel rollouts of multiple services.

System Interdependency Management
Bidders must explain how dependencies and compatibility are managed when systems are deployed together or in sequence.

Configuration & Customization Alignment
Bidders must describe any shared tools or processes (e.g. rule engines, configuration templates) that reduce customization effort.

Time-to-Value Acceleration
Bidders must provide evidence from previous multi-component implementations showing average implementation time savings (absolute value or percentage) compared to standalone deployments (e.g. deploying all Central Bank Gateway System components together along the Messaging Hub as opposed to individual deployments). In addition, Bidders must provide a Work Breakdown Structure (WBS) of the proposed implementation approach (e.g. based on RUP or similar framework), clearly distinguishing between configuration of existing product capabilities and bespoke development.

9.2 Unified Support & SLA

9.2.1 Single Ticketing/Escalation

Centralized support process and SLA across systems reduce handoffs and resolution delays.

SLA Commitments Across Systems
Bidders must define SLA commitments covering the full suite of components (e.g. Gateway, Formatting, Orchestration components within the Central Bank Gateway System and the Messaging Hub). The response must explain how the SLA framework addresses the integration or interdependence between components to ensure coordinated issue resolution, end-to-end service continuity, and consolidated SLA reporting.

24/7/365 Multi-System Support Hours
Bidders must specify whether unified support hours are provided for all systems and confirm the availability of 24/7/365 coverage across the entire solution stack. Any differences in coverage by system, support tier, or region must be clearly outlined.

Onsite & Remote Support Integration
Bidders must describe their support delivery models for multi-component environments, including how remote and onsite assistance is coordinated across product teams, and whether escalation tiers are unified across all systems.

Unified Incident Ticketing System
Bidders must confirm whether a single support portal or ticketing system is available for both systems and explain how multi-component incidents are triaged and resolved across internal product teams.

9.2.2 Coordinated Change/Incident Management

Bidders must demonstrate the ability to align upgrades, patches, and incident response across both systems.

Cross-System Release Frequency & Roadmap
Bidders must describe the frequency of software releases, patches, or regulatory updates across their systems and confirm whether a unified release calendar and roadmap are maintained (e.g. coordinated quarterly updates spanning Financial Message Exchange System and Central Bank Gateway System). The response must include how clients are notified and supported during these updates.

Backward Compatibility Across Systems
Bidders must confirm that backward compatibility is maintained across both systems during upgrades and describe how interoperability and version alignment are ensured.

Vulnerability & Issue Response Coordination
Bidders must describe their process for identifying, patching, and communicating critical bugs or vulnerabilities across multiple components, including client notification procedures and alignment of patch timelines.

Integrated Change Management Tools
Bidders must describe the tools or services they provide to coordinate change management across systems (e.g. shared test environments, rollback plans, coordinated patch validation).

10 Qualification and Other Relevant Requirements

10.1 General Eligibility Criteria

This RFP is open to solution providers with demonstrated expertise in:

- Design and implementation of financial Messaging Hub for central banks or national payment infrastructures, and/or Messaging Gateway solutions with equivalent functionality for financial institutions or payment infrastructures.
- ISO 20022-compliant messaging, transformation, and orchestration.
- Secure, scalable, and high-availability financial infrastructure solutions.
- Integration with messaging networks, payment gateways, and external market infrastructures.

In addition to meeting the above eligibility criteria, each Bidder must also satisfy the following qualification requirements.

10.2 Bidder's Qualification Criteria

Messaging Service Deployments
Bidders must demonstrate successful deployments of messaging solutions within central bank infrastructures, financial market infrastructures, or other regulated payment systems. Bidders are encouraged to provide deployment references along with details of the project scope and clients served.

Deployments in Comparable Regulatory Environments
It is desirable for the Bidder to have experience deploying solutions in countries with regulatory environments comparable to Armenia, particularly in emerging markets and mid-tier digital economies with similar compliance and reporting requirements. For the Messaging Hub, preference will be given to deployments in jurisdictions using their own domestic network rather than SWIFT. Bidders are encouraged to provide relevant market examples to demonstrate this experience.

Interoperability Messaging Experience
It is desirable for the Bidder to have extensive experience with domestic or cross-border messaging, formatting, orchestration infrastructure deployments, including integration with SWIFT networks, correspondent banking relationships, and international clearing systems. Demonstrated experience with large-scale, complex environments, including high message volumes, broad participant networks, wide geographic scope, and strong performance metrics for transaction processing and settlement, will be considered an advantage.

Long-Term Client Relationships
The Bidder must demonstrate strong client retention over 3+ years with major financial institutions, showing evidence of successful contract renewals, service expansions, technology upgrades, and continuous partnership value. Bidders must provide examples of long-term engagements including client testimonials, retention rates, and evidence of successful platform evolution within existing relationships.

Project Failures or Security Incidents
Bidders must disclose any publicly known project failures, legal disputes, or security incidents including data breaches or operational disruptions, along with resolution outcomes and lessons learned. Preference is given to those with no unresolved incidents or ongoing contractual disputes.

10.3 Account Management and Project Team Qualification Requirements

Account Management, Governance, and Executive Engagement
Bidders must maintain a skilled account management team with structured governance models and executive-level client engagement. Clear organizational structure, team qualifications, and governance frameworks implemented for similar clients must be described in detail.

The bidder must demonstrate the capability to provide a qualified, experienced, and well-structured team to ensure effective project delivery, governance, and executive-level client engagement.

Qualified Project Personnel
The bidder must allocate qualified and experienced personnel capable of fulfilling all contractual obligations and ensuring that project objectives (timeline and quality) are achieved.
Team members involved in the implementation must have demonstrated experience executing similar large-scale projects with relevant technical, managerial, and domain expertise required for the project.
As evidence of compliance, the bidder must submit CVs[4] of all key experts, including supporting documentation confirming qualifications and certifications;

Language and Communication Requirements
All team members must have at least working proficiency in English.
Knowledge of Armenian and Russian is desirable.

10.4 Financial Standing

Financial stability
Bidders must present evidence of their financial stability over the last 3 years and forecast for 2026,

[4] *Where Bidders submit personal data as part of their Proposal (e.g., CVs, diplomas, certificates), the Central Bank of Armenia will process such data solely for the purposes of conducting and evaluating this procurement procedure and performing any resulting contractual obligations.*

The CBA will handle personal data lawfully, fairly, and securely, ensuring its confidentiality and using it only for purposes related to this procedure. Personal data will be retained only for the statutory period required for procurement records and will be securely deleted or archived thereafter.

By submitting such data, the Bidder confirms that it has obtained all necessary permissions or has a valid legal basis for providing this personal data to the CBA.

demonstrating consistent financial performance, liquidity, and capital adequacy to sustain long-term contractual obligations. The required evidence shall include, at a minimum:

- International network audited financial statements for the last three fiscal years (2022, 2023, and 2024). Audited financial statements must be issued by an independent audit firm applying internationally recognized auditing standards. If requested audited financial statements are not available, unaudited financial statements must be provided;
- Interim financial statements or management accounts for 2025;
- Banking references or letters from financial institutions confirming the Bidder's financial soundness, resilience, and ability to meet long-term contractual commitments.

All documents submitted must be clear, complete, and issued or signed by authorized entities (auditors, financial institutions, or rating agencies). The CBA reserves the right to request additional clarification or supporting documentation as needed.

10.5 Financial Proposal Requirements

10.5.1 Cost & Licensing

Bidders shall provide a detailed description of the proposed licensing model and corresponding pricing. The proposal must also indicate any modular licensing options, separate pricing for additional components or features, and the Central Bank's ability to scale or adjust license usage over time without contractual penalty.

Upfront Licensing Costs
Bidders must specify the upfront licensing costs associated with the proposed Financial Message Exchange System and / or Central Bank Gateway System. Bidders should also provide details of any relevant pricing tiers, thresholds applicable to the licensing structure.

Implementation Cost Breakdown
Bidders are required to submit a detailed breakdown of the total implementation cost. This should include all activities necessary to operationalize the Financial Message Exchange System and / or Central Bank Gateway System, such as software configuration, system integration, customization, project management, testing, and support during the deployment phase. In addition to listing all required licenses (e.g. Operating Systems, MS Queries), Bidders must also provide the corresponding licencing costs for these components. Each component should be described with sufficient clarity to demonstrate how the cost relates to the project scope.

Ongoing Support and Maintenance Costs
Bidders must outline the annual costs associated with support and maintenance of the deployed solution over a minimum period of 10 years. This should include standard support charges, upgrade entitlements, security patching, bug fixes, version enhancements, SLA commitments, and delineation between what is covered under standard versus premium support tiers. Bidders must also clearly delineate the scope and pricing of standard vs premium support tiers, ensuring that long-term maintenance and upgrade obligations are fully covered within the proposed support model.

Infrastructure Requirements and Associated Costs
The Bidder must provide a clear summary of the hardware, storage, network, and operating system requirements to deploy the solution. The proposal must distinguish between primary and disaster recovery environments and state whether the Bidder offers cloud or on-premises deployment options. If cloud deployment is proposed, it should primarily be positioned for testing, non-critical, or lower-tier environments. Associated costs for each infrastructure model should be outlined clearly, including third-party software licenses if applicable.

Modular Licensing Structure
Bidders must specify whether the licensing allows modular acquisition of features, such as separate licensing for reporting modules. The proposal must state whether these modules can be licensed independently or only as part of a bundled suite.

Licensing for Non-Production Environments
Bidders should indicate their standard approach to licensing for non-production environments (test, development, training, disaster recovery). This information is requested for evaluation purposes only and final terms will be subject to negotiation.

Cost Breakdown and Transparency
An itemized cost sheet must be provided that includes all software license fees, professional services, testing environments, infrastructure requirements, documentation, and any additional costs expected to be incurred during implementation or support phases.

Visibility of Future Costs
Bidders must describe the mechanisms used to ensure predictability of future costs. This includes projected expenses for future upgrades, new features, user expansion, or institution onboarding. Bidders should explain how such changes are priced and how customers are informed of pricing impacts in advance.

10.5.2 Cost Efficiencies and Bundled Pricing

Multi-system offerings are expected to deliver pricing advantages across licensing, implementation, and support (in case of proposing both Lot 1 and Lot 2 solutions).

Licensing Costs
Bidders must specify whether systems are offered under a bundled pricing scheme and outline fee structures. Any bundled discounts or pricing tiers must be quantified.

Implementation Costs
Bidders must provide a detailed breakdown of implementation costs for the integrated suite, including integration work between systems and customization. Any bundled discounts should be explicitly stated.

Support & Maintenance
Bidders must provide details of ongoing support and maintenance costs and clarify whether support services are bundled across systems or priced separately. SLA coverage and unified support provisions must be described.

Infrastructure Requirements & Cost
Bidders must outline infrastructure requirements for multi-system deployment, including opportunities for shared environments (e.g. all Central Bank Gateway System components and Messaging Hub running on a shared platform). Pricing for shared infrastructure must be provided, with comparison across cloud vs on-premises options and any third-party dependencies.

Future Cost Visibility
Bidders must explain how their pricing model accounts for long-term cost drivers, including user growth, regulatory updates, or additional modules. The response must demonstrate how multi-system usage impacts predictability of future costs.

Deployment Flexibility
Bidders must describe whether multiple system can be deployed in a shared containerized or virtualized environment, including implications for resource consumption, security isolation, and scalability.

Operational & Monitoring Tools
Bidders must confirm whether centralized observability, monitoring, or incident management tools are offered across systems and quantify any operational savings or efficiencies enabled by such shared capabilities.

10.6 Source Code Escrow Requirements

Source Code Escrow Agreement
Bidders must specify whether a source code escrow agreement will be provided for the proposed solution or not. The response should detail the frequency with which source code is deposited or updated, ensuring alignment with software release cycles.

Escrow Agent and Security
Bidders are required to identify the escrow agent used, including whether a third-party service is engaged. The proposal must provide information on the agent's reputation, reliability, and security measures in place to safeguard the deposited materials.

Escrow Agreement Structure
Bidders must confirm whether the escrow arrangement will be established as a tripartite agreement among the buyer, the bidder, and the escrow agent. The proposal should emphasize that such a structure is considered the most secure option.

Escrow Release Conditions
In case of Escrow Arrangement, bidders must define the conditions that would trigger release of the escrowed source code. These may include, but are not limited to, bidder insolvency, cessation of support, breach of contractual obligations, or failure to deliver agreed-upon services. The response

should outline the process for invoking and executing such a release. Otherwise, the Bidder must specify alternative procedures that ensure the continued availability and operation of the solution.

11 Implementation / Delivery

11.1 Proposed Implementation Roadmap

The Bidder shall provide a clear, integrated, and practical roadmap for the implementation of the service.

The roadmap must cover the full project lifecycle from contract signing to final go-live while accounting for interdependencies between the Financial Message Exchange System and the Central Bank Gateway System components. Specifically, the roadmap must include:

- A proposed implementation and delivery plan of key activities for each system (e.g. change analysis, development, configuration, integration, installation, testing, commissioning, readiness acceptance, go-live, after care), and an indication of whether a parallel or sequential deployment is proposed
- A proposed methodology and approach to identify gaps, configuration definitions and integration specifications including templates used, with explicit reference to how these align with the organization's SDLC (Software Development Life Cycle) and governance framework
- A description of the development and configuration change management process and version controls, aligned with CMMI Capability Maturity Levels (CML) to demonstrate process maturity, governance, and continuous improvement
- A rationale for the proposed sequence, including any benefits, the identification of delivery, technical, and operational risks with clear mitigation strategies, demonstrating proactive risk management, governance, and contingency planning
- A proposed master test plan describing the tests performed by individual parties or combined, with alignment to SDLC quality gates and integration checkpoints
- A proposed training plan, knowledge management and documentation plan must be provided to support the capture and transfer solution specific knowledge and documentation
- A tentative timeline showing estimated durations and key milestones, with clear identification of:
    - Gap & Change Assessment
    - Delivery timelines for Development, Configuration and Integration checkpoints between components and/or systems
    - Environment readiness dates
    - Testing and training phases
    - Final acceptance and operational readiness & transition
- A list of prerequisites, dependencies, and required inputs from the CBA and/or third-party vendors, including infrastructure provisioning, data readiness, technical resourcing, and institutional coordination

The roadmap must support overall project planning, stakeholder alignment, and readiness tracking. It must be included in the Bidder's proposal and may be accompanied by a high-level Gantt chart or equivalent planning tool to illustrate proposed workstreams, timelines, and dependencies.

If the Bidder is submitting a proposal for only one system, the roadmap must clearly explain how interoperability with the other system will be achieved during the implementation.

11.2 Implementation & Support

Training Approach and Coverage
Bidders must offer a comprehensive training plan including classroom, virtual, on-the-job, and e-learning methods. The training program should be adaptable to the Central Bank's operational and regulatory context with the specific scope, extent, and level of customization to be finalized during contract negotiation and the implementation phase.

Localized Training
Training materials must be localized and tailored to the central bank's specific implementation configuration and business processes. Materials must be available in Armenian where required and incorporate relevant local payment system examples and operational procedures specific to the Armenian market context.

Knowledge Transfer Strategy
Bidders must provide a detailed knowledge transfer plan enabling Central Bank teams to independently operate and maintain the system post-implementation. The plan should cover documentation with clear roles, timelines, and mechanisms to validate knowledge retention.

Support Availability
The solution must provide full 24/7/365 support, including during holidays and critical windows such as end-of-day processing, settlement cycles, and other high availability periods. Scheduled maintenance windows may be allowed but must be agreed in advance with the Central Bank and designed to minimize operational impact.

Remote and Onsite Support Options
Bidders must describe support delivery models, including local presence capabilities, remote escalation paths, and scheduled onsite check-ins. The support model must include provisions for emergency onsite/offsite assistance within defined timeframes and local language support capabilities where required. This requirement must be covered by the price of the 10-year SLA.

Release Frequency and Roadmap Sharing
The Bidder must demonstrate a structured product development lifecycle with regular updates delivered at least annually, including feature enhancements, performance improvements, and regulatory compliance updates.

Backward Compatibility of Releases

All new software releases must maintain full backward compatibility with existing configurations, interfaces, and data structures without requiring major system migrations or operational disruptions. Bidders must describe their compatibility testing processes, regression testing procedures, and rollback capabilities. Any breaking changes must be clearly identified with detailed migration paths and extended transition periods.

Realistic Delivery Timeline

Bidders must propose a realistic delivery timeline that accurately reflects project complexity, organizational readiness requirements, testing phases, and integration dependencies. Unrealistic commitments will be penalized. Timelines must include realistic allowances for user acceptance testing, parallel running, and staff training with appropriate contingency buffers.

Change Management and Version control

Bidders must provide a description of how the application development/evolution is managed in terms of delivering upgrades, how user requirements and market practice changes are incorporated into product evolution, and how version and quality control is implemented to ensure error-free deployments.

Governance RACI Matrix

Bidder must deliver a RACI matrix covering all activities: development, integration, testing, deployment, cutover, acceptance, and post-go-live support.

12 Deliverables

12.1 Expected Deliverables and Planned Timelines

The planned timelines are for guidance only. Bidders must submit, in their proposals, a detailed schedule for contract execution, specifying all key phases and their respective target completion dates.

EXPECTED DELIVERABLES	PLANNED TIMELINES
• Delivery and Deployment of the System - All modules are installed, configured, and integrated.	• Up to XX 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 XX months
•	•
• Pilot operation - Critical and key workflows are executed and demonstrated by real users.	• Up to XX months
• Final Delivery and Acceptance of the System	• Up to XX months
• Warranty period	•
• Technical Support and Maintenance	• In line with the timeline provided in the proposal

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

12.2 Project Documentation

The Bidder shall create and maintain all project documents that shall be passed on to the CBA as deliverables as per the agreed project timelines and WBS. The documents created by the Bidder will be reviewed and approved by the Central Bank.

The stages, activities, and corresponding deliverables outlined in the table below are provided for guidance. Bidders must submit, in their proposals, a detailed description of stages, related activities as well as provide corresponding documentation.

Stage	Activities	Deliverables
Project Planning	• Project Planning and Management • Project Quality Assurance • Documentation of Project Plan • Project Status Reporting	• Project Management Plan • Project Acceptance Strategy • Weekly and monthly status reports
Business and Functional Requirements Analysis	• International standards and practice assessment • In-depth analysis of business and functional requirements • Stakeholders need analysis • Document final set of business requirements • Define and document functional requirements	• Benchmark review assessment report • Business Requirement Specification • Functional Requirements Specification • Requirement Validation and Traceability Plan • Software Requirements and Specifications Document
System Architecture Design	• Document a preliminary set of businessrules and workflows • Conceptual architectural system designmethodology • Develop a strategy to ensure a finalintegrated design • Documentation of a comprehensivedesign style guide • Prepare and develop strategy for design session results and validation of these results	• Solution Architecture • Information Architecture • Integration Architecture • Infrastructure Architecture • Security Architecture
Implementation	• Conduct ongoing reviews of the hardware and software performance andreliability to determine if hardware meets service level agreements. • Develop implementation strategy • Certify that the application, its domains, functions, data, processes, operationalprocedures, staffing and all other associated support are in operation • Chart contingency plans • Resolution of all issues • Approval of Project Team to move to the implementation phase of the project	• Application Implementation Plan • Release Notes
Testing and Acceptance	• Develop a strategy for testing the application processes and creating	• Master Test Plan • System integration test case

Stage	Activities	Deliverables
	test environments • Develop criteria for promotion from unit to integration test • Integration Testing • Demonstrate readiness for UAT	• Test Protocol for Unit, Integration, and UAT stages • Performance MonitoringPlan • Performance, Volume and Stress Testing Reports
	•	•
System Maintenance Support and Operations	• Stress Testing • Load Testing • Performance Testing • Make recommendations for changes to hardware or software requirements to improve performance • Documentation of the knowledge transfer materials that will be used toprovide orientation and kick-off for testing • Identification of the tools and reports thatwill be used to support all testing efforts • Steps to ensure any design changes arereflected in the test scripts system • Resolution of all issues identified as design issues • Resolution of all defects that prevent completion of test scripts • System Incident Resolution • Application Enhancements • Minor changes, bug fixes, error resolutions and minor enhancements • Application Upgrades and updates • Apply regular patches	• System Integration Execution Report – on daily basis • System Maintenance and Support Plan • System Incident Resolution report • Adaptive Maintenance Report • Application • Enhancements Report
Training and Knowledge Transfer	• Documentation of the Knowledge Management Strategy • Documentation of the approach for evaluating the effectiveness of the knowledge transfer and training courses or sessions • Documentation of the train-the-trainer strategy	• Knowledge Transfer and Training Plan • Training and Instructional Material • Application User Manual • Online User Aids

Stage	Activities	Deliverables
	• Develop knowledge transfer programand classroom training materials • Conduct Trainings as per the details provided in the ToR • Develop a methodology for reporting, reviewing, and improving knowledge transfer • Collect and monitor training feedback	
Go-Live	• Go-Live	• Decision on Go-live

12.3 Acceptance Criteria

Acceptance will occur once the following conditions are met:

- All functional and non-functional requirements validated
- End-to-end integration tests passed
- DR failover demonstrated
- No Critical/High defects open
- Documentation approved
- UAT completion and sign-off
- Performance benchmarks achieved

13 Acronyms and Definitions

13.1Acronyms

Acronyms	Full Names
ADF	Application Development Framework
AES	Advanced Encryption Standard
AMD	Armenian Dram
AML	Anti-Money Laundering
API	Application Programming Interface
APM	Application Performance Monitoring
ArCa	Armenia Card (Armenia's card provider for Retail Payments)
A2A	Application-to-application
BCP	Business Continuity Plan
BIC	Bank Identifier Code
BIS	Bank for International Settlements
BRICS	Brazil, Russia, India, China, and South Africa
CASB	Cloud Access Security Broker
CBA	Central Bank of Armenia
CBPR+	Cross-Border Payments and Reporting Plus
CCP	Crisis Communication Plan
CD	Continuous Delivery
CDA	Central Depository of Armenia
CI	Continuous Integration
CNAPS	China National Advanced Payment System
CPU	Central Processing Unit
CSD	Central Securities Depository
CSV	Comma-Separated Values
DB	Database
DC	Data Centre

Acronyms	Full Names
DLP	Data Loss Prevention
DR	Disaster Recovery
EAEU	Eurasian Economic Union
EBRD	European Bank for Reconstruction and Development
EPS	Electronic Payment System (CBA's current RTGS)
EU	European Union
FAQs	Frequently Asked Questions
FMI	Financial Market Infrastructure
FIPS 140-3	Federal Information Processing Standard 140-3
GDPR	General Data Protection Regulation
GRC	Governance, Risk, and Compliance
GSASS	Government Securities Accounting and Settlement System
HA	High Availability
HSM	Hardware Security Modules
HVPS+	High-Value Payment System Plus
IAAS / IaC	Infrastructure as a Service / Infrastructure as Code
IEC	International Electrotechnical Commission
IMF	International Monetary Fund
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IRP	Incident Response Plan
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO20022-AM / ISO-AM	The ISO 20022 Usage Guideline for Armenia
ISO 22301	International Standard for Business Continuity Management
ISO/IEC 27001	International Standard for Information Security Management

Acronyms	Full Names
ISO/IEC 27036	Information Security for Supplier Relationships
JSON	JavaScript Object Notation
JWS/JWT	JSON Web Signature / JSON Web Token
KPI	Key Performance Indicator
KRIs	Key Risk Indicators
KYC	Know Your Customer
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEI	Legal Entity Identifier
MFA	Multi-Factor Authentication
MT/MX	Message Types (SWIFT messaging standards)
NBFI	Non-banking financial institutions
NICs	Network Interface Cards
NIST	National Institute of Standards and Technology
OIDC	OpenID Connect
OKRs	Objectives and Key Results
OS	Operating System
OTP	One-Time Password
OWASP	Open Worldwide Application Security Project
PAM	Privileged Access Management
PCI DSS	Payment Card Industry Data Security Standard
PFMI	Principles for Financial Market Infrastructures
QA	Quality Assurance
RA	Republic of Armenia
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-based access control
RCA	Root Cause Analysis

Acronyms	Full Names
RFP	Request for Proposal
ROI	Return on Investment
RTGS	Real-Time Gross Settlement
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RUP	Rational Unified Process
SAN	Storage Area Network
SAML	Security Assertion Markup Language
SBOM	Software Bill of Materials
SEPA	Single Euro Payments Area
SFMS	Structured Financial Messaging System (India)
SFTP	Secure File Transfer Protocol
SIEM	Security Information and Event Management
SIT	System Integration Testing
SLA	Service Level Agreement
SMEs	Small and Medium-sized Enterprises
SOAR	Security Orchestration, Automation, and Response
SOC 2	System and Organization Controls (Type 2)
SPFS	System for Transfer of Financial Messages
SSDLC	Secure Software Development Life Cycle
SSH	Secure Shell
S&F	Store-and-Forward
STIX	Structured Threat Information Expression
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SWIFT FIN	SWIFT Financial Messaging Network
TAXII	Trusted Automated eXchange of Indicator Information
TLS	Transport Layer Security

Acronyms	Full Names
UAT	User Acceptance Testing
UETR	Unique End-to-End Transaction Reference
UN	United Nations
U2A	User-to-application
VAT	Value Added Tax
WAN	Wide Area Network
WBS	Work Breakdown Structure
XBRL	eXtensible Business Reporting Language
XML	Extensible Markup Language
XSD	XML Schema Definition
2FA	Two-Factor Authentication

13.2 Definitions

Acronyms	Full Names
CBANet	The CBA operates a global communication network CBANet - functions as a large Layer 3 (L3) infrastructure, fully administered and maintained by the CBA. CBANet is designed for financial institutions functioning within Armenia. Financial information traffic is transmitted between subscriber endpoint devices and the central node devices. Subscriber endpoint devices are installed at the premises of the respective institutions and are connected to their local area networks. The central nodes are located at CBA sites and aggregate information flows from all subscribers.
Technical Validation	Validation against a technical schema (e.g. XSD)
Message Validation	Cross-field validation in a message, comparable to Swift's Network Validation
Business Validation	Validation of the message in the specific business context, e.g. a payment message (pacs.008) can only be processed if there are sufficient funds in the account
Delivery	Delivery is the fundamental process of transferring data / information from a source system to a destination system. Example: transferring data from the Messaging Gateway to the Messaging Hub

Acronyms	Full Names
Routing	Routing is the process of selecting the most suitable destination system (CBA Internal System) for the data / information to be processed by, based on specific criteria. Selection criteria are 1. 5-digit Destination Bank Identifier, 2. Business Service and 3. Message Type
Orchestration	Orchestration is the process of coordinating multiple steps, (potentially) involving both delivery and routing, to achieve the processing of a message. Flow Orchestration enables involved parties to view at an initiated instruction (via submitting a messaging) end-to-end
BankMail	The Financial Messaging System, which is currently in use

General Terms & Conditions (T&Cs)

DISCLAIMER:

(The Bidder(s) acknowledge and agree that this Public General Terms and Conditions ("General T&Cs") published by Central Bank of the Republic of Armenia ("CBA") in this Announcement shall form an integral part of any agreement, contract, or purchase order resulting from this tender process and shall not be subject of negotiation and/or revision by Bidder(s).

If the selected Bidder(s) refuse to include these General T&Cs in the formal contract with CBA, or otherwise impede their inclusion, such refusal will be considered a rejection to enter into the contract in accordance with the Law of the Republic of Armenia on Procurement.)

1. Upon the award of the tender and execution of the formal implementation and deployment contract(s) (hereinafter "Contract") between Central Bank of the Republic of Armenia (hereinafter "CBA") and selected Bidder(s) (hereinafter also "Contractor(s)"), the General T&Cs shall automatically be deemed incorporated into, and made binding upon, the parties as though fully set forth in the Contract.
2. The Contractor(s) shall perform services under Lot 1 (Financial Message Exchange System) and/or Lot 2 (Central Bank Gateway System) strictly in accordance with General T&Cs, this Tender announcement, RFP and another relevant documents that are published, attached or referred by this Tender announcement ("Documentations").
3. The CBA accepts the following licensing model for Lot 1 (Financial Message Exchange System) and/or Lot 2 (Central Bank Gateway System):
   (a) Perpetual License or Similar License.
   The Contractor(s) grants the CBA a perpetual, irrevocable, transferable (in the territory of the Republic of Armenia), and royalty-free license to use, install, and operate the software for the purposes prescribed by Documentations.
4. The Contractor(s) represents and warrants that the software, license and the use thereof by the CBA, does not and will not infringe or misappropriate any copyright, patent, trade secret, trademark, or other intellectual property or proprietary right of any third party.
5. The Contractor(s) shall indemnify, defend, and hold harmless the CBA, its affiliates, officers, employees, and agents from and against any and all losses, damages, liabilities, costs, and expenses (including reasonable attorney's fees) arising out of or relating to any claim, demand, or action by a third party alleging that the software infringes or misappropriates such third party's intellectual property rights. In the event of any such claim, the Contractor(s) may, at its own expense and discretion:
   a) procure for the CBA the right to continue using the software;
   b) replace or modify the software so that it becomes non-infringing without materially affecting its functionality; or

c) if neither (a) nor (b) is commercially reasonable, terminate the license, service and refund to the CBA the prepaid fees for the remaining unused term.

6. The Contractor(s) grants the CBA a right to configure, and integrate the provided software with the CBA's internal systems, databases, and third-party applications, for the purpose of enhancing functionality or interoperability, provided that such customization or integration:
    a) does not infringe upon any third-party intellectual property rights;
    b) is performed solely for the CBA's business purposes prescribed by Documentations; and
    c) does not result in the creation of a competing software or service.
7. The Contractor(s) and the CBA shall attempt to settle any dispute resulting from the execution of the Contract amicably. Any disputes shall be subject to the exclusive jurisdiction of the London Court of International Arbitration. Any dispute, controversy, or claim arising out of or in connection with this Contract, including any question regarding its existence, validity, interpretation, performance, breach, or termination, shall be referred to and finally resolved by arbitration under the LCIA Rules, which Rules are deemed to be incorporated by reference into this clause. The seat (legal place) of arbitration shall be London, England. The number of arbitrators shall be 1 (one) arbitrator. The language of the arbitration shall be English. The governing law of the Contract shall be the substantive law of laws of the Republic of Armenia.
8. The Contractor(s)' and the CBA's liability is limited to the value of the Contract. Any other limitation of liability for parties shall not apply, until expressly agreed by the CBA.
9. In the event, when Contractor(s) acts as vendor, distributor or agent of another company (producer company), which owns the license/software, the Contractor(s) shall remain fully responsible to the CBA for all obligations set out in the Documentations and Contract. Nevertheless, nothing in these General T&Cs shall limit the CBA rights to claim against not only the Contractor(s) but also the producer company, in its discretion.
10. CBA and/or Contractor(s) can assign, mortgage, charge, or sub-license their rights only with written consent of the other party.
11. Nothing in the Contract shall prohibit the Contractor(s) from granting licenses and the CBA from obtaining similar licenses/software with respect to the service and the software to other third parties.
12. If the Contractor(s) provide Escrow agreement, at least the following trigger events shall apply:
    a) the Contractor(s) is liquidated or otherwise dissolved; an order is made for the winding up of the Contractor(s), or the Contractor(s) passes a resolution for winding up or is wound up whether compulsory or voluntarily (other than for the purposes of a solvent reconstruction or amalgamation); or the Contractor(s) has a receiver appointed over all or any part of its assets or

undertaking; or the Contractor(s) becomes the subject of any business rescue proceedings or an administration order, or enters into any composition or arrangement with its creditors; or any similar or analogous proceedings or event occurs in respect of the Contractor(s) within the relevant jurisdiction;

b) The Contractor(s) files a voluntary petition or otherwise seeks relief under any bankruptcy, insolvency, or similar law;
c) The Contractor(s) has been declared bankrupt or has been granted suspension of payments, either by involuntary or voluntary proceedings.

13. Where the Contract refers to terms and conditions available on websites, the Contractor(s) agrees that only the version of such terms attached to the Contract shall apply. Future changes on website shall not apply to the Contract unless expressly approved in writing by the CBA. In the event of any conflict, inconsistency, or ambiguity between such terms and conditions, and the Documentations, the Documentations shall prevail and govern.
14. The Contractor(s) shall not use, display, reproduce, reference, or otherwise make use of the CBA's name, trademarks, service marks, trade names, logos, branding elements, or any other identifiers ("Marks") in any marketing materials, case studies, press releases, customer lists, presentations, proposals, websites, or any other public communications without the CBA's prior written consent, which may be granted or withheld at the CBA's sole discretion.
15. Contract shall have the following contractual clauses for the termination by the CBA: The CBA shall have the right to terminate the Contract, in whole or in part, by written notice to the Contractor(s), if the Contractor(s):
    a) materially breaches any provision of the Contract and fails to remedy such breach within 15 (fifteen) business days after receiving a written notice specifying the breach;
    b) fails to render/deliver any part of the Lot 1 (Financial Message Exchange System)/Lot 2 (Central Bank Gateway System) during the term of the Contract,
    c) suspends the performance of the Contract for any reason not connected to CBA's fault,
    d) fails to ensure that the software complies with the technical specifications, performance indicators, security requirements, or other criteria set out in the tender Documentations or the Contract, and does not remedy such non-compliance within the period specified in the Contract;
    e) fails to provide maintenance, updates, patches, or support services in accordance with Documentations and the Contract, causing disruption to the CBA's operations or preventing the intended use of the software and does not remedy such scenarios within the period specified in the Contract;

f) delivers software containing repeated, critical, or unresolved defects that materially affect its use, performance, or availability, and does not correct such defects within the timeframe established by the Contract;
g) violates confidentiality, data-protection, information-security, or access-control requirements of the CBA;
h) engages in conduct contrary to applicable law or fails to comply with mandatory regulatory requirements relevant to the performance of the Contract; or
i) through any action or omission, creates a material risk to the CBA's business continuity, system stability, data integrity, or the security of the CBA's IT infrastructure.

In such cases, termination shall become effective upon the date specified in the CBA's written notice, and the Contractor(s) shall be obligated to promptly refund to CBA all payments received (advance, delivery-based, milestone-based payments) at the date of such termination. All such refundable amounts shall be reimbursed to CBA within 15 (fifteen) business days of receipt of written notice from the CBA. The Contractor(s) refund obligation shall apply regardless of any costs incurred by the Contractor(s) and shall be without prejudice to any other rights or remedies available to CBA under this Contract or by law.

T&Cs of Payments and delivery models

16. The total price of the System(s) (including license, software, maintenance, support) provided by Contractor(s) is final and the Contractor(s) cannot impose additional costs for updates, patches, fixes, or required third-party components. The Contractor(s) reconfirms that the CBA shall not pay any additional fee for any feature of the software.
17. The Contractor(s) who submits positive audited financial statements that meet the Purchaser's requirements (see ToR Section 10.4) shall be eligible for the following 3 (three) phased payments.

a) Phase 1 – Advance Payment

Up to 25% of the total Contract value may be paid as an advance payment according to Section 8 of Invitation.

b) Phase 2 – Milestone-Based Payment

The remaining Contract value shall be paid according to a delivery- and milestone-based payment structure, aligned with the approved implementation roadmap.

c) Phase 3 – Go-Live Payment

At least **30% of the total Contract value** shall be paid upon Go-Live.

Phase 2 and Phase 3 payments shall be deemed payable only upon (i) the Contractor(s)' full and satisfactory completion of the corresponding milestone, and (ii) the CBA's written

acceptance of the milestone following any required testing, review, or validation procedures set out in the Documentations.

18. The Contractor (s) who do **not** demonstrate financial standing as described above (didn't submit positive audited financial statements) shall be eligible only for receiving **the total Contract value after Go-Live.** In other words, no advance or milestone payments will be provided, and whole payment shall be made solely upon Go-Live.
19. All payments to the Contractor(s) under the Contract—whether advance, milestone-based, or final—shall be released only upon execution of a mutually signed Act of Acceptance by both parties. No payment obligation shall arise, nor shall any invoice be considered valid for processing, until the relevant Act of Acceptance confirming satisfactory completion of the applicable deliverables, milestones, or obligations has been duly signed by the parties. The payments to Contractor(s) shall be made within 10 (ten) working days after mutual sign off of the relevant Act of Acceptance.
20. Contractor(s) shall be responsible for providing the simulation mechanisms and acceptance tools required to organize and perform acceptance testing independently of the other systems.
21. The deliverable package and acceptance criteria for each implementation stage shall be defined and negotiated on the basis of the work breakdown structure proposed by the Contractor(s) in its RFP response and shall become an integral part of the Implementation Roadmap. The following items constitute a **mandatory, but not exhaustive, list** of deliverables to be included in each package:
    a) the deliverable itself;
    b) a delivery description and complete package inventory;
    c) test reports, including internal functional, non-functional, and regression (where applicable) testing;
    d) simulation mechanisms and acceptance tools required to organize and perform acceptance testing independently of the other system components or Lots;
    e) load test reports (where applicable);
    f) vulnerability assessment and penetration testing protocols (where applicable);
    g) deployment and configuration instructions;
    h) integration points configurations instructions - documentation and functional connections to existing systems and external parties (where applicable);
    i) migration instructions (where applicable);
    j) internal and external user guides (where applicable);
    k) IT support manuals and operational guides;
    l) training materials and training sessions (where applicable);

m) signed support and maintenance contract (applicable only for the Go-Live).

22. The **acceptance process** shall be formalized and binding for both Parties. The acceptance procedure shall include:
    a) the CBA shall have a formally defined and limited period *(to be agreed and specified in the Contract)* to review and accept each deliverable package;
    b) The CBA shall document all identified comments, defects, and issues as part of the acceptance process'
    c) The Contractor(s) shall have a defined and limited timeframe *(to be agreed and specified in the Contract)* to fix all blocking and critical issues identified during acceptance.
23. If blocking or critical issues are not corrected within agreed and specified timeframe, the respective stage shall be considered not accepted.

T&Cs of Implementation Roadmap.

24. The project roadmap proposed in the RFP response by Contractor(s), as subsequently refined during the negotiation phase and aligned with the final scope of work, actual start and final dates, shall form an integral part of the Contract as the Implementation Roadmap.
25. The Contractor(s) shall be fully responsible and liable for complying with all timelines, milestones, and deadlines set forth in the approved **Implementation Roadmap.** Implementation RoadMap shall be subject to **strict monitoring and control**. The Contractor(s) shall immediately notify the CBA in writing of any circumstances that may affect its ability to meet the agreed deadlines. Such notification shall not release the Contractor(s) from its obligations under the Contract unless expressly agreed to in writing by the CBA.

T&Cs of Penalty Calculations.

26. Any failure by the Contractor(s) to meet the deadlines or milestone dates specified in the Implementation Roadmap—unless caused by Force Majeure or by the CBA's written instruction or CBA's fault—shall constitute a **contractual delay**. In such cases, the Contractor shall be subject to delay penalties. In case of violation of the **Implementation Roadmap** (included interim and final deadlines) by Contractor(s), CBA reserves the right to claim a penalty in the amount of 0.1 (one tenth) per cent of the amount payable at the given stage/phase prescribed by Implementation Roadmap for each overdue day.
27. In case of violation of the payment terms specified in the Contract and upon written request of the Contractor(s), Contractor(s) reserves the right to claim a penalty in the

amount of 0.1 (one tenth) per cent of the amount payable at the given stage/phase prescribed by Implementation Roadmap for each overdue day.

28. The CBA's decision not to immediately impose penalties shall not be construed as a waiver of its right to enforce the penalty provisions at any later time.
29. The imposition of delay penalties shall be without prejudice to any other rights or remedies available to the CBA under the Contract.
30. The CBA has a right to make direct deductions of penalties from the payments payable to Contractor(s).

T&Cs of Project management Governance

31. The Contractor for the Lot 2 (Central Bank Gateway System) shall be responsible for executing all integration activities required to ensure seamless interoperability between the Central Bank Gateway System and the Financial Message Exchange System, as well as with SWIFT.
32. **Operational-Level Meetings**. The Contractor(s) shall organize regular operational-level meetings, held no less frequently than once every two weeks, to update the CBA on the current status of work, plan upcoming activities in detail, and highlight any emerging issues or risks. The CBA may request additional operational-level meetings when reasonably necessary, including in response to urgent issues, changes in scope, or material risks.
33. **Steering-Level Meetings.** The Contractor(s) shall organize regular steering-level meetings, held no less frequently than once every month, to inform the Project Sponsor and Product Owner on project progress and to address any issues or risks that cannot be resolved at the operational level.
34. The Contractor(s) shall ensure the attendance of personnel with appropriate technical and managerial authority to address operational matters, resolve issues, and make necessary decisions. The Contractor(s) shall prepare and circulate relevant materials, including progress reports, updated schedules, risk assessments, and any other documentation reasonably required by the CBA prior to each meeting.
35. The Contractor(s) shall not transfer, assign, or otherwise delegate its responsibilities, obligations, or deliverables under the Contract to any third party, whether in whole or in part.
36. In all circumstances, the Contractor(s) shall remain fully accountable to the CBA for the satisfactory and timely performance of all deliverables under the Contract, irrespective of any assistance obtained from third parties.

T&Cs of Support and Maintenance

37. The Contractor(s) shall provide 12 (twelve) month warranty for each System (Lot 1 Financial Message Exchange System and/or Lot 2 Central Bank Gateway System) starting from Go-Live date ("Warranty Period").
38. During this Warranty Period, the Contractor(s) shall, at no additional cost to the CBA, perform all necessary repair and corrective actions required to restore the relevant System to the level of functionality existing on its respective Go-Live date.
39. Contract should include a clause, that parties agree to sign a separate support and maintenance contract. Support and maintenance contract shall include the availability of all essential functions of each System, updates, security patches, technical support, documentation, and interoperability measures necessary to maintain each System in good working order.
40. The support and maintenance contract will be signed for a minimum of 10 (ten) years starting from Go-Live.
41. The support and maintenance contract shall include
    a) fixed pricing for the first 3 (three) years, with procedures for price revision for each next 3 (three) year's period with up to 20% adjustment limit (compared to the previous period price),
    b) minimum support service levels and maintenance conditions

    consistent with those proposed in the Contractor(s)' RFP submission.
42. The Contractor(s) and the CBA shall attempt to settle any dispute resulting from the execution of the support and maintenance contract amicably. Any disputes shall be subject to the exclusive jurisdiction of the London Court of International Arbitration. Any dispute, controversy, or claim arising out of or in connection with the support and maintenance contract, including any question regarding its existence, validity, interpretation, performance, breach, or termination, shall be referred to and finally resolved by arbitration under the LCIA Rules, which Rules are deemed to be incorporated by reference into this clause. The seat (legal place) of arbitration shall be London, England. The number of arbitrators shall be 1 (one) arbitrator. The language of the arbitration shall be English. The governing law of the support and maintenance contract shall be the substantive law of laws of the Republic of Armenia.

Appendix 2

Tender Invitation

Reference Number: CBA-2025-062

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

APPLICATION-STATEMENT

For participation in RFP

_____[Name of Bidder or in case of JV, insert legal name of each member]]

wishes to participate in

□ Lot 1 only

□ Lot 2 only

□ Both Lots 1 and 2

of the RFP with Reference Number CBA-2025-062, 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 where the conviction has been removed or extinguished in accordance with the law.
   c) We have not allowed and will not allow anti-competitive agreements, unfair competition, or abuse of dominant position during our participation in this procedure.

d) There is no simultaneous participation of any affiliated person, 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.
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 deadline for submission of proposals specified in the announcement and remains valid until the event specified in clause 9.4 of the Invitation.
4. If we are selected as the selected bidder, we undertake to provide contract security in accordance with the Invitation and to deliver the services within the timeframes specified in the Technical Task.
5. In accordance with clause 3.3 of this Invitation, we confirm that we are not submitting more than one proposal to this tender process.
6. We understand that this bid, if selected, constitutes a binding contract between us and the Purchaser until a formal contract is prepared and executed.

1) Name of Bidder:	*[insert Bidder's legal name], or [In case of JV, insert legal name of each member]*
2) Legal Address:	*[insert Bidder's legal address in country of registration], or [In case of JV, insert legal address in country of registration of each member]*
3) Business Address (if different):	*[insert Bidder's business address in country of registration], or [In case of JV, insert business address in country of registration of each member]*
4) Taxpayer Identification Number:	*[insert Bidder's Taxpayer identification number] or [In case of JV, insert Taxpayer identification number of each member]*
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:	

Appendix 2.1

Tender Invitation
Reference Number: CBA-2025-062

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/**	**Passport Series, Number/**	**Amount of Share Ownership**

			Date of State Registration	**State Registration Number**	
	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					
11.	Provide information about the members of the organization's executive body.				
	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:				
	First Name, Last Name	**Citizenship**	**Date of Birth**	**Passport Series, Number**	**Position**

** 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.

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) _____---

(date of birth)

c) _____---

(citizenship)

b) _____---

(passport series/number)

†† 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.).

	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		
1.	Does the organization have a compliance practice?	Yes □ No □
	If yes, please provide contact information: 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?⌗	

⌗ 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.

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:	

Appendix 3
Tender Invitation
Reference Number: CBA-2025-062

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-2025-062, _[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 ten-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 Bidders 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. In case of signing a contract with a non-resident Bidder 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 bidder 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, USD or EUR (in numbers and words)	VAT AMD, USD or EUR (in numbers and words) (if applicable)	Total Price AMD, USD or EUR (in numbers and words)
1	***2***	***3***	***4***	***5=3+4***
1	Financial Message Exchange System	{in numbers}	{in numbers}	{in numbers}
		{in words}	{in words}	{in words}
2	Central Bank Gateway System	{in numbers}	{in numbers}	{in numbers}
		{in words}	{in words}	{in words}

_____ _____

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

Appendix 3.1

Tender Invitation
Reference Number: CBA-2025-062

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)

[The Bidder shall submit a detailed breakdown of the System supply and implementation costs for each lot separately, clearly specifying the unit and total prices for each proposed component, including terms, schedule, and procedure for payment. An advance payment may be granted only if the Bidder submits positive audited financial statements that meet the Purchaser's requirements (see ToR Section 10.4)]

Comp. Nr	Name	Brief description	Meas. Unit	Qty	Unit Price, incl. VAT (if appl.) /AMD, USD or EUR/	Total Price Incl. VAT (if appl.) /AMD, USD or EUR/
1	*2*		*3*	*4*	*5*	*6 =4x5*
1.						
2.						
…						

Detailed warranty service terms _____

Payment Terms _____

Payment Conditions _____

_____ _____

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

Appendix 3.2
Tender Invitation
Reference Number: CBA-2025-062

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 Post-Implementation recurring Costs)

[The Bidder shall provide a separate breakdown using Annex 3.2 of the expected post-implementation costs, for each lot separately. The Bidder must outline the annual costs associated with support, maintenance and other required expenses of the deployed solution over a minimum period of 10 years. Clearly outline the payment terms, schedule, and procedures. If pricing is exposed to foreign exchange volatility, the Bidder must clearly specify the applicable terms and risk-sharing arrangements.
For each category, the Bidder shall also provide a 10-year cost projection, indicating key drivers of future cost changes (e.g. number of participants, transaction volumes, regulatory updates) in line with ToR Section 10.5.]

No	Name	The annual price of the service period per year					Total Prices
		Year 1	Year 2	Year 3	Year	Year 10	*AMD, USD or EUR*
1	.....						
2	.....						
3	.....						
4	.....						
Annual Subtotals:							
VAT (if applicable) /AMD, USD or EUR/							
Cumulative total cost of expenses							

Post-implementation recurring costs will be used exclusively for evaluation and comparison purposes in calculating the Total Cost of Ownership (TCO). A separate contract for the post-implementation period will be concluded after the implementation phase, taking into account the following terms:

- *Contract signed for a minimum of ten (10) years;*
- *Fixed pricing for the first three (3) years;*
- *The agreed procedure and frequency of price reviews for each next 3 years, including 20% adjustment limits.*

Terms, schedule, and method of payment _____

Detailed terms of post-warranty service _____

_____ _____

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

In addition to Appendices 3, 3.1, and 3.2, the bidder shall submit a completed detailed cost breakdown in XLS for each lot. The bidder must populate the sheet titled *"Financial Msg Exchange System"* in the file *CBA-2025-062_Appendix_3_1.xlsx* for Lot 1, and the sheet titled *"Central Bank Gateway System"* in the same file for Lot 2.

Appendix 4

Tender Invitation
Reference Number: CBA-2025-062

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

COMPREHENSIVE DESCRIPTION
of the Proposed Solution

_____[Name of Bidder]_____ presents below a comprehensive description of the Solution proposed by bidder within the framework of the Tender with Reference Number CBA-2025-062, broken down by component.

The Bidder shall structure the technical part of its Proposal in line with the Terms of Reference (Appendix 1), explicitly covering all chapters.

For each requirement, the Bidder shall clearly indicate compliance, partial compliance or non-compliance and provide supporting explanations.

The technical proposal shall also include: an implementation RACI matrix in line with ToR Section 11, a cutover and rollback strategy aligned with the CBA's operational requirements, and a high-level Business Continuity and Disaster Recovery concept consistent with ToR Chapter 8 and Chapter 6.

A detailed description of the proposed solution shall contain the following populated Vendor Response documents and use file name "CBA-2025-062_Appendix_4":

- "CBA-2025-062_Appendix_4_Lot_1"* and/or
- "CBA-2025-062_Appendix_4_Lot_2"*
- and "CBA-2025-062_Appendix_4_Synergies", if the bidder responds to both Lot 1 and Lot 2 and
- Documents describing the proposed solution (e.g. Architecture Diagrams, Integration Diagrams, Project Plans, User Guides) using file names "CBA-2025-062_Appendix_4_Attachment _[dd]" where [dd] reflects a sequential number used to uniquely identifying each document.

- Implementation timeline showing durations and key milestones
- Any other documents and information specified in Terms of Reference of this Invitation,

Note that for certain requirements stated in documents CBA-2025-062_ Appendix_4_Lot_1 .xlsx and CBA-2025-062_ Appendix_4_Lot_2.xlsx, respondents are asked to select their Delivery Approach. A selection must be done in column "Delivery Approach" when the current selected value states "(Please select from below)*". The respondent can select between the following values:

- *Requires product development* – to be used when the current product does not support the requirement and the Respondent intends to develop and include the required functionality as part of future product development. Example: the product does not support the manual entry of payment messages and the Respondent plans to add this functionality in a future release.
- *Requires customization for CBA* – to be used when the current product partially supports the requirement, and the Respondent plans to deliver the required functionality through customization of the existing product. Example: the product supports manual entry of payment messages but does not implement the 4-eyes principle, which the Respondent plans to add as a customization for CBA.
- *Comes out of the box / configuration* – to be used when the requirement is fulfilled by functionality that is readily available in the product or can be implemented through standard configuration.

Further explanations shall be provided in the "Vendor Response" column. The Respondent may refer to additional documents included in its submission (please refer to cipher e) above), by specifying the file name in the "Attachment Name" column. If multiple documents are referenced, the file names shall be separated by commas.

Attachment Name	Content Description

Appendix 5

Tender Invitation

Reference Number: CBA-2025-062

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

INFORMATION

About the Bidder's "Professional experience"

[In addition to the minimum participation requirements and minimum qualification requirements defined in Clause 2 of this Invitation, the Bidder must also meet the qualification criteria set out in the Terms of Reference.
Bidders shall demonstrate proven experience in the design and implementation of messaging solutions for central banks, financial market infrastructures, or other regulated payment systems, including evidence of client relationships maintained for at least three (3) years.
The submitted portfolio shall include information on successfully implemented systems within the last three (3) years prior to the submission date.
The Bidder shall also provide Client confirmation or supporting reference materials (e.g., reference letters, project briefs, regulator acknowledgements, or publicly available information) validating successful completion.]

№	Name of Partner Organization and country	Project scope and key objectives / Brief Description	Implementation timeline and duration Month/Year	Main solution components and technologies used	Dedicated team/team size in the whole Project	Approximate value of the contract /AMD, USD or EUR/	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:

Appendix 6

Tender Invitation

Reference Number: CBA-2025-062

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

INFORMATION

About the Bidder's "Human Resources"

[The Bidder shall provide an Organizational and Governance Overview that includes the organizational structure of the proposed account management and project team, CVs or profiles of key personnel, a description of the governance and decision-making framework (including escalation and communication procedures), and examples of similar client engagement models implemented for other central banks or financial institutions.

The Bidder shall assign qualified and experienced personnel to perform the required tasks and ensure the achievement of the Contract objectives in terms of both timeline and quality. All personnel involved in the project implementation must possess the necessary qualifications and demonstrated experience in similar projects to ensure high-quality performance.]

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

** As evidence, the Bidder must submit the CVs of key personnel (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 or Armenian (knowledge of Russian is desirable).*

Where Bidders submit personal data as part of their Proposal (e.g., CVs, diplomas, certificates), the Central Bank of Armenia will process such data solely for the purposes of conducting and evaluating this procurement procedure and performing any resulting contractual obligations.

The CBA will handle personal data lawfully, fairly, and securely, ensuring its confidentiality and using it only for purposes related to this procedure. Personal data will be retained only for the statutory period required for procurement records and will be securely deleted or archived thereafter.

By submitting such data, the Bidder confirms that it has obtained all necessary permissions or has a valid legal basis for providing this personal data to the CBA.

Key Personnel Details

Position		**Candidate** ☐ **Prime** ☐ **Alternate**	
Personnel information	**Name**		
	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