



ՀՀ կենտրոնական բանկ

ՀԵՏԱՔՐՔՐՈՒԹՅԱՆ ՀԱՐՑՈՒՄ

**Հայաստանի ֆինանսական շուկայի
ենթակառուցվածքի արդիականացում
(Նոր սերնդի հաղորդագրության
համակարգ և RTGS-ի փոխարինում)**

Կոնտակտային տվյալներ

Հայաստանի Կենտրոնական Բանկ

Վազգեն Սարգսյան փողոց 6

Երևան, 0010, Հայաստան

Էլ. հասցե: eps-info@cba.am



Table of Contents

1	Executive Summary.....	3
1.1	What is Being Procured.....	3
1.2	Why It's Important	3
1.3	Who Can Respond	3
1.4	Impact	3
1.5	Desired Outcome.....	3
2	Introduction.....	4
2.1	Purpose of this REol.....	4
2.2	About Armenia Financial Sector.....	4
2.3	About the Central Bank	5
2.4	Overview of the Functions of the Central Bank.....	5
2.5	Operational Status of the Central Bank	6
2.6	Objective of the Project.....	6
2.7	Project Stakeholders	8
2.8	REol Protocol	10
2.9	Questions & Answers	10
2.10	Management Cast / Industry Briefing.....	11
2.11	Structured Response Template for Vendors	11
3	Envisaged Future State	12
3.1	Business View.....	12
3.1.1	Functional Requirements.....	12
3.1.2	Non-Functional Requirements.....	17
3.1.3	Business Functions / Processes.....	18
3.2	Logical View.....	20
3.2.1	Technical Components	20
3.2.2	Technical Infrastructure check.....	23
3.3	Deliverables.....	27
4	Appendix	28
4.1	Acronyms & Definitions	28



1 Executive Summary

1.1 What is Being Procured

The Central Bank of Armenia (CBA) is initiating the modernization of its Financial Market Infrastructure (FMI). This Request for Expression of Interest (REoI) invites qualified vendors to express their interest in delivering one or both of the following critical components:

- A Financial Messaging System consisting of Messaging, Orchestration and Formatting services – note that vendors, which are only experienced in one or two of the three services, are invited to express their interest for the specific service
- A Real-Time Gross Settlement (RTGS) System

These solutions must meet international standards, particularly ISO 20022, and support real-time & store-and-forward, secure, and scalable transaction processing within Armenia's financial system.

1.2 Why It's Important

This strategic modernization aims to:

- Enhance operational efficiency, resilience, and security across national payment infrastructures
- Align with global standards such as the BIS Principles for Financial Market Infrastructures (PFMI) and ISO 20022
- Future-proof Armenia's financial ecosystem for payments, regional integration, and regulatory transparency
- Strengthen interoperability between the CBA, market participants, and international partners

1.3 Who Can Respond

This REoI welcomes vendors with proven expertise in:

- Secure, scalable, and high-availability financial infrastructure platforms
- Financial messaging gateways
- Central bank or national-level RTGS systems
- ISO 20022 transformation
- As well as interoperability with global systems such as SWIFT

Vendors may respond for one or both components or for one or more subcomponents of the Financial Messaging Gateway outlined in chapter 1.1. Responses should demonstrate technical capability, relevant experience, and implementation readiness.

1.4 Impact

The outcome of this REoI will shape the next phase of Armenia's financial market infrastructure. Vendors will be invited to participate in an RFP process, forming the foundation of a multi-year transformation journey. This is a rare opportunity to work with a forward-looking central bank on a strategically critical initiative.

1.5 Desired Outcome

The vendors participating in this REoI will deliver a completed response form covering the solution including solution architecture, implementation and timeline. They will also deliver supporting evidentiary documentation where possible and a high-level estimation of the delivery, implementation, licensing and ongoing support costs to the CBA in USD (\$).



2 Introduction

2.1 Purpose of this REoI

The purpose of this Request for Expression of Interest (REoI) is to invite qualified vendors and solution providers to formally express their interest in participating in the upcoming procurement process for the modernization of Armenia's national financial market infrastructure, including the implementation of a next-generation financial messaging system and the replacement of the Real-Time Gross Settlement (RTGS) system.

This REoI serves to identify experienced, capable, and innovative firms with proven expertise in financial infrastructure projects, particularly in ISO 20022-based messaging, real-time settlement systems, and secure, scalable architectures.

Important Notice: This REoI is non-binding and is issued solely to assess vendor capabilities, interest, and readiness. Vendors are welcomed to submit any pricing, system designs or solution architectures at this stage. Vendors will be invited to respond to Requests for Proposal (RfP) in the next phase, where detailed functional, technical, and commercial offers will be evaluated.

2.2 About Armenia Financial Sector

As of 2024, Armenia's financial system is composed primarily of 17 commercial banks, 9 insurance companies, 43 credit organizations and 22 investment companies. The banking sector continues to dominate the financial landscape, with total assets reaching AMD 10.5 trillion (approximately USD 26.4 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.

Total bank loans amounted to AMD 6.1 trillion (approximately USD 15.4 billion), while deposits rose to AMD 7.3 trillion (around USD 18.4 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 Central Bank of Armenia (CBA) remains the primary regulator, overseeing commercial banks, insurance, securities, credit organizations, and payment systems. Continued regulatory reforms and digital transformation initiatives such as e-wallet integration, real-time payments, and open banking infrastructure have significantly improved financial inclusion. The fintech sector is rapidly growing, supported by innovation hubs and favourable regulations.

Non-bank financial institutions (NBFIs) especially in microfinance and SME lending continue to play a vital role, particularly in underserved rural areas.

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 regulatory 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 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, including the IMF, World Bank, BIS, and EBRD, 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 and Inflation Control:** 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, payment system operators, 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.
- **Foreign Exchange and 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. It maintains operational control over a set of national financial infrastructures and is actively modernizing its systems in alignment with international standards.

The CBA currently:

- Manages a functional RTGS system, which supports high-value interbank payments and settlements in central bank money. However, the current platform 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 provides clearing and settlement of non-government issued securities
- Manages GSASS (Government Securities Accounting and Settlement System), which provides clearing and settlement of government issued securities
- Oversees a growing array of non-cash payment systems, including instant payments, card-based ArCa system and mobile payment infrastructures, under its oversight.

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 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 platforms.

2.6 Objective of the Project

The Central Bank of Armenia (CBA) is undertaking a comprehensive modernization of its national financial market infrastructure, with a dual focus on renewing its Real-Time Gross Settlement (RTGS) system and implementing a next-generation financial 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 Modernization:**Modern Financial Messaging System**

This solution will consist of three interoperable services:

- Messaging Service: A secure, standards-compliant platform enabling real-time, system-to-system exchange of financial messages.
- Formatting Service: A configurable engine for validating, transforming, and enriching messages in accordance with AM-HT¹, ISO 20022 (ISO-AM) and SWIFT standard CBPR+.
- An Orchestration Service providing routing to CBA internal systems but flexible enough to be exchanged with or extended to a comprehensive flow orchestration at a later stage.

Renewed RTGS System

The upgraded RTGS system will facilitate (high-value) interbank payments in real time, support payment message prioritisation, advanced liquidity management, other RTGS specific functionalities, and improve the CBA's oversight capabilities. Replacing the legacy platform – operational since the early 2000s and constrained by monolithic architecture – the new RTGS will feature modular design, high availability, and native support for ISO 20022 standards.

Strategic Goals:

- Ensure high levels of system availability, performance, and security.
- Support real-time processing with advanced liquidity, credit risk, and messaging controls.
- 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 both the RTGS and gateway environments.
- Establish a foundation for future capabilities such as high-value interbank instant payments, enhanced regulatory reporting, and regional integration.
- Improve interoperability with domestic systems (e.g. Core Banking, General Ledger, Integration Layer, Control Centre, Central Data Store), SWIFT, regional platforms, 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. Vendors may propose solutions for one or both components (Financial Messaging System and RTGS) or services of the Financial Messaging System, but interoperability, seamless integration, and long-term extensibility will be key evaluation criteria, where customization of existing implementations or off-the-shelf solutions is preferred over a bespoke solution.

¹ Messaging format which is currently used in Armenia (see *Acronyms & Definitions*)

Հայաստանի ֆինանսական շուկայի ենթակառուցվածքի արդիականացում
հաղորդագրության համակարգ և RTGS-ի փոխարինում

(Նոր սերնդի



By undertaking this modernization, the CBA positions itself to meet growing demands in terms of transaction volumes, regulatory expectations, and cross-border interoperability² – ensuring the long-term stability and innovation readiness of Armenia’s national Financial Market Infrastructure.

2.7 Project Stakeholders

This Request for Expression of Interest (REoI) supports the future modernization of the Central Bank of Armenia’s (CBA) national financial market infrastructure – specifically the implementation of a new Financial Messaging System and the replacement of the Real-Time Gross Settlement (RTGS) system.

The success of this modernization depends on effective coordination among a diverse group of internal and external stakeholders. Vendors are expected to operate in a collaborative environment and align with the roles outlined below:

Internal Stakeholders

- Steering Committee (SteerCo): Provides strategic oversight, validates key decisions, and ensures alignment with the CBA’s long-term digital roadmap. Vendors may be invited to present at major project milestones.
- CBA Senior Management: Sets overall direction and ensures consistency with institutional priorities, including resilience, compliance, and innovation.
- Procurement and Vendor Management Unit: Leads transparent and competitive procurement processes. Responsible for vendor onboarding and contracting.
- Payment Services and Data Governance Center (PSDGC): Serves as the primary interface for vendors on technical and functional aspects, coordinating solution assessments, implementation, testing, cross-party and vendor coordination, and representing end users and operational processes. Also supports requirements gathering, change management, and user onboarding activities as well as performance monitoring throughout the project lifecycle.
- IT Architecture & Infrastructure Teams: Evaluate technical proposals for alignment with CBA’s enterprise architecture, including containerization, security, and scalability.
- Information Security and Cybersecurity: Ensures that all components of the modernized infrastructure adhere to strong security standards, such as threat detection, vulnerability management, incident response, and compliance with relevant regulations. Provides ongoing security monitoring, coordinates penetration testing, and manages responses to cyber incidents.
- Market Operations: Proceed with Account Management and Financial Markets (Securities & FX) services
- Risk, Compliance & Internal Audit: Ensure all vendor solutions comply with regulatory, cybersecurity, and data protection standards. Involved in reviewing SLAs, risk mitigation plans, and business continuity strategies.

External Stakeholders

- Market Participants: Includes commercial banks, financial institutions, and other users of the RTGS and messaging systems. Expected to participate in readiness activities, such as message validation, connectivity testing, and onboarding.
- External Vendors & Integration Partners: May contribute expertise in areas such as system integration, data migration, testing, and third-party interface certification. Collaboration will be key to ensuring successful end-to-end delivery.

² cross-border interoperability refers to the support of the Swift Tracker, i.e. for cross-border payments sent thru the domestic MI notifications are sent to the Swift Tracker



Respondents to this REoI 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.



2.8 REol Protocol

All communications and submissions related to this Request for Expression of Interest (REol) must follow the timelines and procedures outlined below:

- REol Issuance Date: *20 August 2025*
- Question & Answer sessions for vendors: *bilaterally upon request until 24 September 2025*
- Assumed REol Submission Date: *26 September 2025*
- Additional clarification meetings: *until 10 October 2025*
- Invitation to participate in the RfPs: *November / December 2025*

Submissions shall be sent electronically to eps-info@cba.am

Central Bank of Armenia (CBA) appreciates that vendors will conform to the format and structure defined in the *Structured Vendor Response Template* document.

As an outlook for the forthcoming RfP the Central Bank of Armenia (CBA) already wants to share the following eligibility conditions in accordance with the Law on Procurement of the Republic of Armenia:

Ineligible Participants

- Have been declared bankrupt by a court
- Have been convicted (within the last 5 years) of terrorism financing, child exploitation, human trafficking, bribery, or other crimes related to economic activity (unless expunged)
- Have a final administrative ruling against them for anti-competitive behavior, abuse of dominant position, or unfair procurement practices within the last 3 years
- Are on the Eurasian Economic Union (EEU) blacklist (unless this procurement is funded under an international agreement)
- Are on Armenian procurement blacklists
- Affiliated persons or entities, including those founded by the same individuals or having more than 50% joint ownership, may not participate simultaneously, unless through a formal joint venture (JV)

The subsequent tender will include:

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

2.9 Questions & Answers

Interested vendors may submit written questions or requests for clarification regarding this REol by the specified deadline. All questions must be submitted to the official contact point:

Contact: eps-info@cba.am

Answers to all received questions will be compiled and shared with all interested parties via email, to ensure a transparent and level playing field. The Central Bank reserves the right to group and anonymize similar questions.



2.10 Management Cast / Industry Briefing

To support vendor understanding of the project scope and expectations, the Central Bank of Armenia (CBA) may host an optional industry briefing or management presentation.

Date: 27 August 2025 14:30-16:30

Format: Virtual and In-person

Virtual: [EPS Modernization - ROel. Briefing and open Q&A session](#)

<https://us02web.zoom.us/j/81593882733?pwd=ycltuLp56dbkKIGRhQEmFQbTaWPan7.1> or

Meeting ID: 815 9388 2733

Passcode: 520716

In-person: Central Bank of Armenia, 6 Vazgen Sargsyan Street, Yerevan, 0010, Armenia

Participation: Open to all interested vendors

Purpose: To provide strategic context, clarify project objectives and address general queries

2.11 Structured Response Template for Vendors

To support a consistent and efficient evaluation process, vendors are kindly requested to structure their REol response using the response document provided with this REol. The template is intended to provide clarity on what information the Central Bank of Armenia (CBA) seeks to gather at this stage of the procurement process.

3 Envisaged Future State

The final state of Armenia's financial market infrastructure shall be achieved via a multi-year transformation journey starting with the upgrade of the Messaging and RTGS functionality in the first iteration.

3.1 Business View

To seamlessly migrate Central Bank's various services to the future architecture in a fast-pacing environment the new platform shall be built upon pluggable services. This allows for upgrading other functions at most suitable time but also ensures that new services or instruments like tokenized assets can be added at any time.

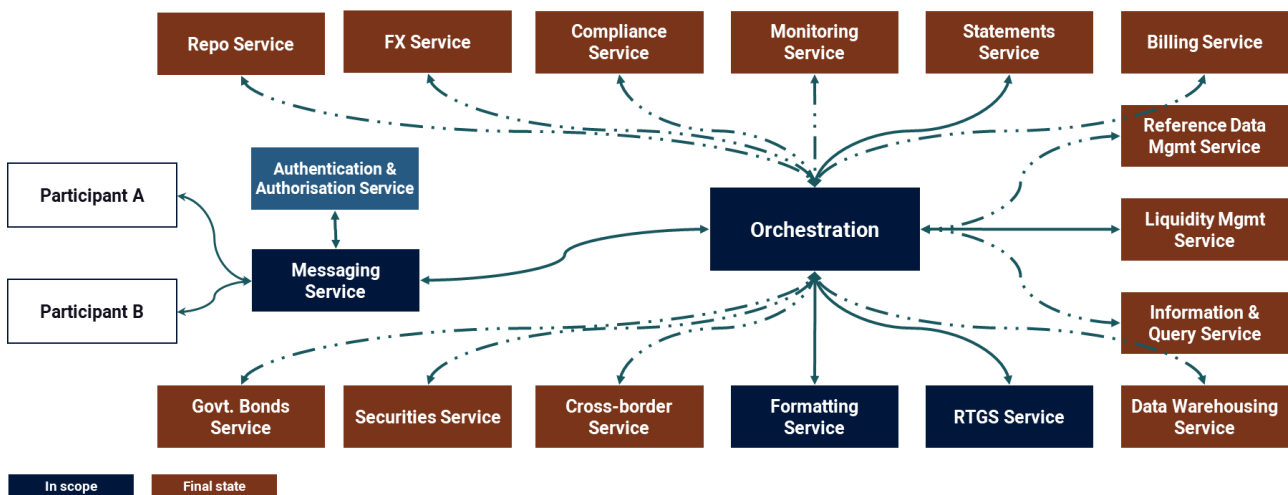


Figure 1: Business view on the financial market infrastructure

In scope of this REol are

- Messaging Service
- Orchestration
- RTGS Service
- Formatting Service

3.1.1 Functional Requirements

The proposed platform must support secure and seamless exchange of financial messages between market participants and the Central Bank as well as among market participants. All messages received by the Central Bank must be routed to relevant downstream systems (e.g. RTGS), with appropriate responses returned to originators and to other involved parties when required. The Central Bank will act as an intermediary, not a processor, of the message content.

The platform must ensure compatibility with the Central Bank's Market Practices and Standards—aligned with ISO 20022 and international best practices — and support dual-format messaging using AM-HT and ISO 20022. Compatibility with the AM-HT format shall be achieved through an HT-XML format that wraps legacy AM-HT messages in ISO 20022 envelopes, supported by a Central Bank adapter.

The platform shall meet all functional requirements outlined below:



3.1.1.1 Messaging Service Functional Requirements

3.1.1.1.1 Message Standards

ISO 20022 & Format Support: Support for payment related ISO 20022 (ISO-AM) messages, including structured fields and dual-format compatibility with AM-HT.

Schema Management: Handle schema versioning, XSD validation, and support coexistence of multiple schema versions.

3.1.1.1.2 Messaging Communication

Connectivity: Provide market participants with guideline documentation and technical libraries and SDKs where needed to connect and interact with the Messaging Hub.

SLA Monitoring & Retry: Monitor SLA adherence and apply automated retry mechanisms with escalation triggers.

Message Replay & Resubmission: Allow replay and resubmission of messages with original timestamps.

Lifecycle State Management: Provide full message lifecycle tracking (received, validated, submitted, etc.) with search and audit support.

3.1.1.1.3 Interoperability

SWIFT Integration: Certified interoperability with Alliance Access, FileAct, InterAct, and services including BIC validation, GPI, and sanctions checks.

Support for other PMIs: Flexibility to support other PMIs to which the Central Bank wants to connect in the future, including full message compliance, FX conversion, and fallback routing.

3.1.1.1.4 Operational Capabilities

Delivery Assurance: Guarantee delivery with commit-confirm protocols, deduplication, and persistence.

Message Storage & Traceability: Provide configurable retention (e.g. 5+ years) including an archiving function, compression, and lifecycle-based purging.

Monitoring & Dashboards: Real-time dashboards with alerting for failures, delays, and SLA breaches.

Logging & Reporting: Maintain timestamped logs and performance reports with administrative event history.

Operational Analytics: Offer real-time KPIs (e.g. throughput, retries) and configurable dashboards for operational insight.



3.1.1.2 Orchestration Service Functional Requirements

3.1.1.2.1 Routing & Orchestration

Dynamic Routing: Route messages based on business / routing rules and support configurable routing logic based on the information available from message's Business Application Header.

Orchestration: 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.

3.1.1.3 RTGS Service Functional Requirements

3.1.1.3.1 Settlement & Liquidity

Real-Time Settlement: Process payments individually and instantly with no batching.

Transaction Finality: Confirm and record settlement irreversibly and in real time.

Scheduling & Reprocessing: Intelligent queuing with retry options based on time or liquidity triggers.

Deferred & Scheduled Payments: Support for future-dated transactions and rule-based scheduling.

Offsetting & Liquidity Optimization: Automatically net and settle offsetting payments to reduce liquidity burden.

Multi-Currency Capability: Track and settle in multiple currencies in real time.

Account Validation & Funds Check: Validate account status and funds availability during processing.

3.1.1.3.2 Risk, Compliance & Oversight

Risk Management: Monitor and enforce thresholds for credit, liquidity, and operational risk.

PFMI Compliance: Full compliance with BIS PFMI principles for FMIs.

Regulatory Oversight Tools: Include built-in stress testing and reporting tools for oversight.

3.1.1.3.3 Operational Features

Security & Compliance: Comply with ISO/IEC 27001 support MFA, RBAC, and audits.

Alerts & Notifications: Real-time notifications based on thresholds or system events.

Reporting & Analytics: Generate real-time and scheduled reports with dashboards.

Logging & Reporting: Maintain audit logs of availability, failover, and recovery events.

Audit Logging: Capture all user/system activity in tamper-proof logs.



Usage Metrics: Track platform usage across users and transaction types.

Search & Inquiry: Support real-time querying of transaction history and statuses.

Monitoring & Dashboards: Provide real-time visibility via dashboards with alerting for failures, delays, and SLA breaches for Central Bank operators.

Logging & Reporting: Maintain timestamped logs and performance reports with administrative event history.

Operational Analytics: Offer real-time KPIs (e.g. throughput, retries) and configurable dashboards for operational insight.

Real-Time Payment Tracker: Enable end-to-end tracking of payments with timestamps, status and reason codes.

Authorization Workflows: Multi-level approval with role-based controls and audit trails.

Access Control: Role-based access for all user types and modules.

Instant Payments Readiness: API and architecture support for future instant payments integration.

Billing & Invoicing: Usage-based billing with customizable rate structures and external integration.

3.1.1.4 Formatting Service Functional Requirements

3.1.1.4.1 Message Format Coverage

Legacy & Custom Format Handling: Ingest AM-HT, batch files (CSV/Excel), and custom XML/JSON with configurable mappings.

Comprehensive ISO 20022 Support: Full support for payment related messages with transformation and enrichment, which can be later extended to securities-related messages.

Multi-Currency & ISO Variant Translation: Enable processing of various currencies e.g. RUB, RMB and translate between ISO variants and national formats.

Mapping, Enrichment & Audit: User-configurable mapping with enrichment tools, audit trails, and rollback capabilities.

Update & API Readiness: Support ISO updates and expose JSON APIs for transformation services.

3.1.1.4.2 Transformation Logic

Message Enrichment: Enrich message fields (e.g. UETR) based upon data stored in Central Bank internal systems with the flexibility of configuring access to such systems and maintain full audit traceability.

User-Friendly Mapping Tools: Provide a no-code/low-code UI for defining transformation logic.



Advanced Logic Support: Support complex mapping structures with conditional logic and custom types.

Reusable Logic Components: Support access to centralized modules for functions like currency conversion.

Context-Based Rules: Apply transformation rules based on metadata (e.g. BIC, country).

Version Control & Auditability: Track changes to mapping templates with rollback and permission controls.

Diagnostics & Logging: Log transformation activity and integrate with monitoring tools.

3.1.1.4.3 Message Validation Rules Engine

Message Validation: Apply context-aware and user-defined message validation rules with detailed error feedback on validation failures and maintain full audit traceability.

Market Practice Rule Packs: Include CBPR+ rules with version management.

ISO 20022 Governance Toolkit: Tools for managing validation rules, updates, and structured overrides.

Real-Time & Batch Validation: Support validation at scale for both real-time and batch processing.

Transparent Error Reporting: Provide actionable error logs with rule-level detail

3.1.1.4.4 Integration Capabilities

API Support: The Formatting Service shall be reachable via API.

3.1.1.5 Integration Functional Requirements

3.1.1.5.1 General Integration Requirements

Web-based Portal: Integrate administration and monitoring functions provided by the components and CBA Internal systems via a Web Portal accessible by both Central Bank users and market participant users. The access shall base upon a standardised implementation approach, which allows to add further functionality at a later stage

AML/CFT Integration: Integrate with AML/CFT screening systems with low-latency response.

Sanctions Screening: Integrate with real-time sanctions screening systems with low latency response.

Reconciliation Integration: Enable ISO-compliant integration with reconciliation systems.

Regulatory Reporting Support: Format and route reports (ADF, XBRL, ISO) per jurisdictional needs.

Monitoring & Audit: Provide logs, alerts, and retries across all integration touchpoints.

3.1.2 Non-Functional Requirements

The Messaging and RTGS Services must meet strict non-functional requirements to ensure continuous availability, real-time performance, resilience, and operational stability. These requirements apply across all environments and deployment models and are critical to ensuring regulatory compliance and uninterrupted operations in a mission-critical financial infrastructure context.

Proposed solutions must demonstrate scalability, fault tolerance, low-latency responsiveness, and automated recovery across containerized and orchestrated platforms. Vendors shall be required to provide evidence of compliance with the criteria outlined below.

3.1.2.1 NFRs applicable to all services

3.1.2.1.1 Performance & Reliability

High & Scalable Throughput: Must support processing of 12,000+ ISO 20022 messages per hour (approximately 90% payments and 10% securities), including nested and large-format structures, with proven performance benchmarks.

Low Latency: End-to-end message latency must remain consistently low during peak loads. Vendors must provide benchmark data and influencing factors (e.g. message size, network conditions).

Scalability & Orchestration: The solution must scale horizontally using containerized services under orchestration (e.g. Kubernetes), with dynamic resource allocation.

High Availability & Disaster Recovery: Built-in clustering, automated failover, and disaster recovery must be supported with RTO under 1 hour and near-zero RPO.

Monitoring & Bottleneck Detection: Real-time monitoring of CPU, memory, and network usage, with alerting and automated remediation for performance bottlenecks.

Stress Resilience: Platform must recover smoothly under extreme load. Vendors must provide validated stress test results.

Graceful Degradation: Must implement circuit breakers, bulkheads, and retry logic to maintain core operations under strain.

Latency Monitoring: Real-time dashboards must track latency, throughput, and errors, with vendor-defined thresholds and test evidence.

3.1.2.1.2 Resilience & Availability

SLAs & Uptime: Vendors must commit to minimum 98% uptime with SLAs covering monitoring, failover, redundancy, and incident response.

High Availability: Must support continuous operation via clustering and seamless failover during planned maintenance.

RTO & RPO: Must support RTO under 1 hour and RPO under 5 minutes, with full details on backup and replication mechanisms.



Disaster Recovery: Must include geographically separate DR site with real-time or near-real-time sync and full continuity.

DR Testing: DR tests must be performed quarterly, with reporting on test scope, metrics, and certifications (e.g. ISO 22301).

Simulation Environment: Vendors must provide a test environment for validating new messages, formats, and workflows without affecting production.

Automated Failover: Platform must auto-detect failures and trigger recovery without manual intervention.

Fault Isolation: Failures must be contained at component level to prevent systemic disruption. Vendors must describe their isolation strategy.

3.1.2.2 Additional Messaging Service NFRs

Automated Failover & Message Rerouting: Must support real-time failover with automatic message rerouting and zero data loss across redundant infrastructure.

3.1.2.3 Additional RTGS Service NFR

3.1.2.3.1 Scalability & Performance

Continuous Availability: System must support 24/7/365 uptime with no planned downtime and built-in redundancy.

Scalability & Throughput: Must support high transaction volumes, 1,000+ batch uploads, and numerous concurrent sessions without degradation.

Peak Load Processing: Real-time transaction processing must be maintained during peak activity, with support for load balancing and horizontal scaling.

3.1.3 Business Functions / Processes

The platform must support the following processes

3.1.3.1 Automated transfer of Xml-based financial messages among two parties

Automatic exchange and routing of ISO 20022-compliant messages (e.g. pacs.008) via the Messaging Gateway and Messaging Hub.

Messages are validated, signed, and securely delivered between participants through the central infrastructure.

3.1.3.2 Manual capturing of a Customer Credit Transfer

Both business users at participant and CBA side (e.g. non-RTGS entities who have an account with CBA) input payment instructions manually via the web portal interface.

Messages are created as pain.001, pass through authorization steps (4- or 6-eyes principle), and are processed as pacs.008 or as pacs.008 or pacs.004 (Return of Funds) or pacs.002 (Reject payment) by the RTGS Service.



3.1.3.3 Manual capturing of a Financial Institution Transfer

CBA or authorized participant users enter interbank transfer instructions manually for direct credit/debit between RTGS accounts.

These follow a similar approval and transformation process into ISO-standard messages for routing and processing as described in chapter *Manual capturing of a Customer Credit Transfer*.

3.1.3.4 Participant / User Management

Functions include user onboarding, role-based access control (RBAC), credentials management, and assignment of privileges

3.1.3.5 Administration and Monitoring functions

Based upon integration requirement *Web-based Portal* described in chapter 3.1.1.5 the platform shall provide web-based administration and monitoring access for the following functions

3.1.3.5.1 for the Central Bank

- Administer (add, change, delete) reference data related to market participants
- Monitor all activities within the platform
- Search for transactions based upon well-defined search criteria e.g. UETR for single transactions or participant id and time window for multiple transactions
- Export / download search results to a local Excel-/PDF-document

3.1.3.5.2 for Market Participants

- Administer business and IT users including their access rights (add, change, delete) under a given SLA for market participant's users
- Monitor incoming and outgoing transactions (payment)

3.1.3.6 Queries & Reports

The platform shall provide secure, web-based capabilities for users to query operational and reference data, with flexible search criteria and export options. Queries shall support both real-time and historical data access; results must be available in user-friendly formats.

- Query modified data: changed attributes, new values, user, timestamps
- Query system time for synchronization
- Query incoming and outgoing messages with date/time, direction, type, service, and optional filters
- Query reference data for parties or participants, with optional filters

3.2 Logical View

Figure 2 provides a logical view on the components making up the platform. Please note that the solutioning of the technical components may differ from this logical view. For the Legacy Systems the Central Bank will provide an adapter as part of the Integration Layer component. Key functionality of this adapter is to envelop AM-HT messages into an ISO 20022 like envelope (similar to SWIFT's XMLv2 with DataPDU), a.k.a. HT-XML, including a Business Application Header as well as to de-envelop a HT-XML message.

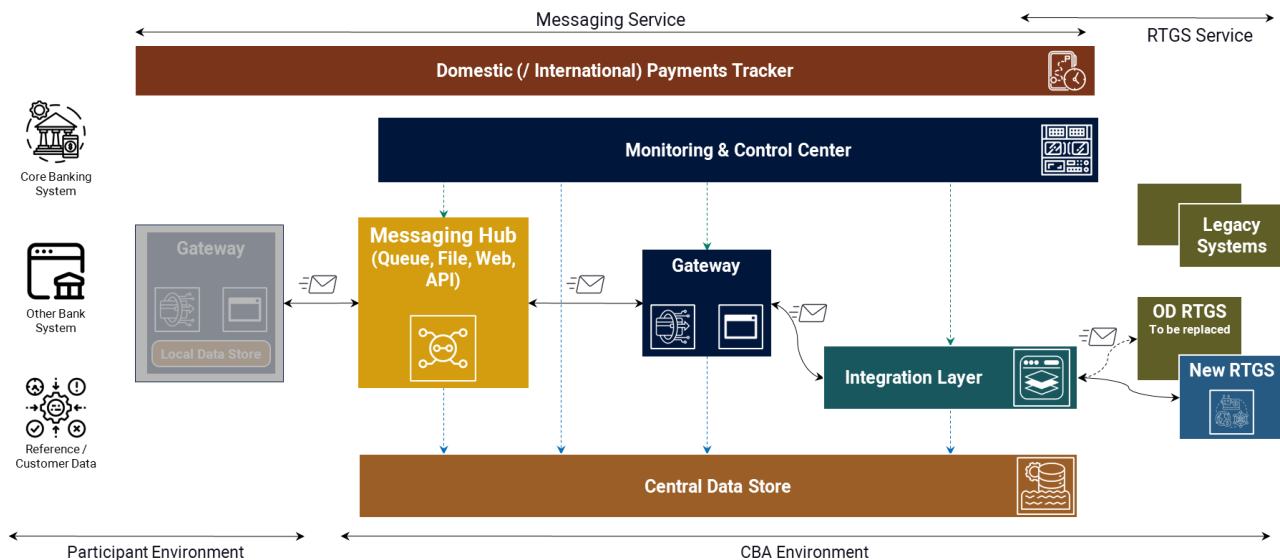


Figure 2 Logical view

The Gateway component depicted in the Participant Environment shall indicate that the Gateway Component used by CBA may be re-used by other market participants. In this case Central Bank expects market participants to use the available Gateway functionality developed for CBA. Central Bank does not intend to provide market participants with a customized version of the Gateway. As per current status Central Bank envisages to provide the market participants with a minimal footprint. This means that the participants will receive guideline documentation about how to connect and interact with the Messaging Service.

3.2.1 Technical Components

3.2.1.1 Messaging Gateway (Access Point)

The Messaging Gateway provides certificate-based access to the Financial Market Infrastructure through CBAnet and allows the Central Bank to send requests via a pre-defined set of channels / protocols. This technical component shall be designed and implemented in a way that participants can use the same functionality in their environment, if needed, where the default gateway option for market participants is described by requirement "Connectivity" in chapter *Messaging Communication*.

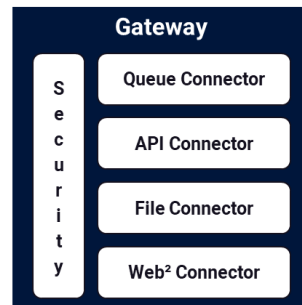


Figure 3 Messaging Gateway Component

Gateway's key functionality is the provision of connectors, where a connector is understood as a technical component or part of such a component that joins the two systems Messaging Gateway and Messaging Hub together. The following connectors shall be part of the Gateway

- Queue Connector – connector allowing the caller to access a technical queue to send or received a message
- File Connector – connector to exchange files with the Messaging Hub component, where files can be transferred via the sftp protocol of (preferably) by making use of either the Queue Connector or the Web Connector
- Web Connector – connector to provide access to the Web Portal of the platform, which logically resides withing the Messaging Hub
- API Connector - connector allowing the execution of API calls, which are logically serviced by the Messaging Hub

3.2.1.2 Messaging Hub

The Messaging Hub shown in Figure 4 is regarded as the central component through which each and any request has to be processed. It holds the endpoints (Queue, File, Web, API) to which a participant sends its requests. Upon reception of the request the Hub performs a technical validation of the request, determines the recipient of the requests, updates the message signature and delivers the message to the receiving party.

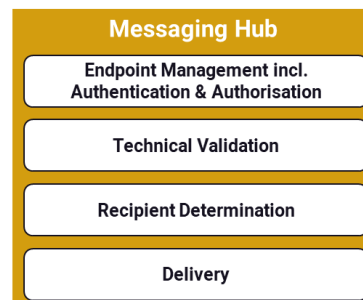


Figure 4: Messaging Hub

If one of the process steps in the Messaging Hub fails, e.g. the technical validation, the Hub is supposed to respond with an appropriate error message, which format shall be aligned with the used protocol standard, which format shall be aligned with the used protocol standard, e.g. an admi.007 message for a message received via the queue endpoint.

3.2.1.3 Orchestration

In its final state the Orchestration depicted in Figure 5 is supposed to be the ultimate core component since this component will be responsible for coordinating multiple steps, (potentially) involving both delivery and routing, to achieve the processing of a message. This means that Orchestration enables involved parties to view at an initiated instruction (via submitting a messaging) end-to-end. Since the upgrade of the financial market infrastructure is conducted in iterations, starting

with the Messaging Service's Go-Live shortly followed by the RTGS Go-Live, a Routing functionality is sufficient for this phase. However, the envisaged Routing Engine is supposed to either support additional functionality at a later stage or seamlessly integrate into a Flow Orchestration Engine, which can be an off-the-shelf product, in the future.

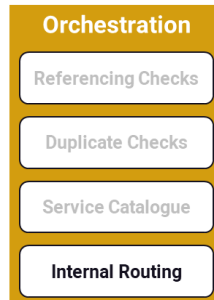


Figure 5 Orchestration

3.2.1.4 Formatting Component

The Formatting component depicted in Figure 6 provides the functionality required to deal with different messaging guidelines and standards. In the beginning the ISO20022-AM standard needs to be supported, which may soon be extended to CBPR+ for cross-border payments. For each supported ISO20022 standard this service shall conduct a message validation based upon the corresponding usage guidelines. In the beginning a validation for an ISO20022-AM message based upon the Armenian ISO 20022 message guidelines is planned.

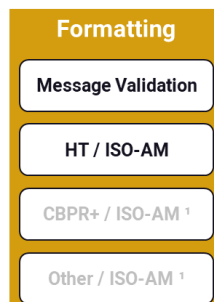


Figure 6 Formatting

Next to the message validation function the service shall also provide functionality for converting messages from one standard to another. In the beginning only a conversion from AM-HT to ISO-AM and vice versa is required.

3.2.1.5 Monitoring and Control Center

The Monitoring and Control Center function shall allow Business Operations and IT Operations to monitor the current status of the platform and its components. In addition the platform is used by Central Bank internal staff to interact with the components for the purpose of configuring them or manually initiating processes. Furthermore, the function shall be used for investigations and issue resolutions by internal staff.

3.2.1.6 Payment Tracker

The Payment Tracker aims to provide both the Central Bank and the market participants with the a visualisation of transactions' current status. This function is comparable to the Swift Basic/gpi Tracker function offered by Swift to its customers.

3.2.1.7 Central Data Storage

The central data storage is used to store any kind of data related to the use of the platform.

3.2.2 Technical Infrastructure check

3.2.2.1 Technology & Architecture Requirements

Respondents are invited to express their capabilities in delivering a modern, secure, and scalable technical architecture to support the Central Bank's Messaging, Formatting, and RTGS services. The proposed solution should align with leading industry standards, demonstrate adaptability to evolving regulatory and operational environments, and support modular, containerized, and extensible system design.

Specifically, vendors are requested to provide the following information for each component:

3.2.2.1.1 Messaging Service Technology & Architecture Requirements

3.2.2.1.1.1 Security

Access Control & Permissions: Must support granular RBAC with dynamic permission management and audit logging for all access events.

Custom Roles & Duty Segregation: Enables creation of custom roles to support separation of duties and configurable permissions beyond default role groups.

Encryption in Transit: Enforces end-to-end encryption (TLS 1.2+ / SSH) for all interfaces (e.g. APIs, SFTP). Vendors must specify protocols and key management practices.

Encryption at Rest: All stored data (messages, logs, databases, backups) must be encrypted using strong industry standards (e.g. AES-256) with documented key rotation policies.

Security Standards Compliance: Must demonstrate compliance with ISO/IEC 27001 and local cryptographic regulations, supported by current certifications or audit reports.

3.2.2.1.1.2 Deployment & Architecture

Deployment Flexibility: Supports on-premise, public/private cloud, and hybrid deployments with minimal configuration changes. Vendors must describe supported models and constraints.

Containerization & Orchestration: Supports containerized deployment using Docker with orchestration platforms like Kubernetes or OpenShift, including automated container lifecycle management.

Stateless & Scalable Architecture: Designed for stateless services that enable seamless horizontal scaling and load balancing without downtime.

Horizontal Scaling & Load Balancing: Built-in support for scaling across services and APIs using orchestration tools and container-based deployment.

High Availability & Redundancy: Supports clustering, failover, and geo-redundancy to maintain service availability and rapid recovery.

Dual Data Centres: Enables active-active or active-passive configurations across physically separated sites with real-time synchronization.



Resource Efficiency: Must optimize CPU, memory, and bandwidth usage under dynamic load conditions. Vendors must demonstrate efficiency via benchmark data.

Monitoring & Observability: Integrates with observability tools (e.g. Prometheus, Grafana, ELK) and supports structured logging, tracing, and metrics export.

Extendibility: Must support APIs, plugins, and event hooks for integrating custom business logic without modifying the core system.

CI/CD & IaC Support: Compatible with CI/CD and infrastructure-as-code tools (e.g. Jenkins, Terraform, Ansible) for automated deployment and infrastructure provisioning.

Automated Testing Support: Provides or supports automated test harnesses, mock services, and regression test pipelines for message validation and integration flows.

3.2.2.1.2 *Formatting Service Technology & Architecture Requirements*

3.2.2.1.2.1 *Security*

Encryption & Standards Compliance: Enforces TLS 1.2+ for data in transit and AES-256 for data at rest across all components (e.g. logs, backups, APIs). Vendors must provide encryption policies or supporting documentation.

Role-Based Access & Logging: Supports custom RBAC roles (e.g. editor, auditor) with logging of access attempts, permission changes, and activity for full traceability.

Sensitive Artifact Protection: Credentials, scripts, and transformation rules must be encrypted, versioned, and protected by tamper-evident mechanisms with secure recovery procedures.

Certifications & Data Sovereignty: Vendors must list relevant certifications (e.g. ISO 27001, SOC 2, GDPR) and describe compliance mechanisms with national data protection and sovereignty laws.

3.2.2.1.2.2 *Technical Architecture*

Deployment Flexibility: Supports on-premise, cloud, and hybrid deployments with configuration options for regulatory, latency, and security needs.

Scalability & Resilience: Enables dynamic scaling and rapid recovery via Kubernetes-based orchestration for stateless services. Vendors must describe recovery times and load performance.

Real-Time & Scalable Integration: Supports REST APIs and message queues (e.g. Kafka, RabbitMQ) for high-volume synchronous and asynchronous communication.

Event-Driven Architecture: Enables asynchronous processing through event streaming technologies with guaranteed delivery and full traceability.

Connectors for Core Systems: Offers customizable or out-of-the-box connectors for core banking systems, messaging hubs, and integration layers, with upgrade-safe design.

Extensibility: Supports plug-and-play updates for formats, rules, and connectors via APIs or SDKs without requiring service restarts.



Extensibility & Customization: Provides SDKs and plugin frameworks for business logic customization with low-code/no-code support and safe version management.

Composable Architecture: Designed with reusable, independently deployable services to enable rapid onboarding of new flows, participants, or business rules.

Monitoring & Observability: Includes health checks, error tracking, and metrics with support for Prometheus, Grafana, or equivalent tools. Users can build custom dashboards and alerts.

3.2.2.1.3 RTGS Service Technology & Architecture Requirements

3.2.2.1.3.1 Security

API Security: Implements OAuth 2.0, mutual TLS (mTLS), API gateways, and rate limiting to ensure secure and reliable API exposure.

Secure-by-Design: Applies layered security including encryption, RBAC, data masking, and secure coding practices across all system components.

Cybersecurity Compliance: Demonstrates compliance with NIST, ISO/IEC 27001, PCI DSS (where applicable), and supports independent audit reviews.

Vulnerability Management: Includes proactive patching, rapid vulnerability resolution, and regular internal and external penetration testing.

3.2.2.1.3.2 Technical Architecture

Deployment Flexibility: Supports on-premise, private cloud, or hybrid models with minimal reconfiguration to align with the Central Bank's infrastructure preferences.

Containerization & Orchestration: Enables container-based deployment (e.g. Docker) and orchestration (e.g. Kubernetes) with support for automated scaling and lifecycle management.

Data Sovereignty: Ensures data residency compliance through configurable data hosting settings aligned with national regulations.

Modular Architecture: Built on modular components (e.g. settlement, billing) that support independent deployment and scalability.

Independent Module Upgrades: Modules can be upgraded independently, with rollback options and dedicated test environments for stability assurance.

Runtime Component Replacement: Enables live component replacement via orchestration tools, ensuring near-zero downtime during maintenance.

Configurable Business Logic: Offers low-code/no-code tools to define rules and workflows (e.g. instant payments) without vendor dependency.



RTGS Architecture Alignment: Fully aligned with Central Bank's RTGS architecture, including interface standards, message specifications, and certification requirements.

Standards-Based API Support: Supports REST, SOAP, and ISO 20022 APIs with complete documentation and adherence to relevant financial standards.

Secure Third-Party Integration: Provides APIs for external integrations secured via authentication, authorization, and access control.

Interoperability Layer: Includes API gateway or middleware to manage API versioning, traffic throttling, routing, authentication, and performance tracking.

Incident Detection & Response: Integrates with SIEM solutions for real-time anomaly detection, alerting, and structured incident response workflows.

Redundancy & Fault Tolerance: Ensures full redundancy of critical components with automated failover, traffic rerouting, and fault isolation.

Modular UI Framework: The system's user interface must be web-based and use a modular design (e.g. React/Angular) to support future extensibility of UI components without disruption.

3.3 Deliverables

At this REoI stage, the Central Bank of Armenia (CBA) is not requesting any technical proposals or deliverables. Instead, we aim to identify vendors with the demonstrated capacity to deliver secure, modern, and scalable solutions for either or both of the following components: Financial Messaging System and Real-Time Gross Settlement (RTGS) system.

To help vendors understand the scope and lifecycle of the upcoming project, the table below outlines the indicative categories of deliverables that vendors may be expected to provide during later phases of the procurement process. These deliverables are non-binding at this stage and will be formally defined in the Requests for Proposal (RFP).

Vendors are encouraged to highlight any prior experience delivering similar outputs in relevant Central Bank or similar infrastructure projects.

Stage	Activities	Expected Deliverables
Project Planning	Initial setup Governance definition Workplan	Project Management Plan Status Reports
Requirements Analysis	Stakeholder workshops ISO 20022 alignment Needs assessment	Business Requirements Document Functional Specifications Traceability Matrix
Architecture & Design	End-to-end solution design Security & Infrastructure planning Integration architecture	Solution Architecture Document Security Architecture Integration Design
Implementation Planning	Migration strategy Release schedule Environment setup	Implementation Strategy Release Notes Deployment Plan
Testing	Test strategy System/integration testing Data validation	Master Test Plan Test Reports Data Migration Validation Report
Maintenance & Support	Support model setup Monitoring & patching Incident response planning	System Maintenance Plan Incident Logs Support Documentation
Training & Knowledge Transfer	User onboarding Training development Knowledge handover	Training Materials User Manuals Knowledge Transfer Strategy



4 Appendix

4.1 Acronyms & Definitions

Acronyms	Full Names
ADF	Automated Data Flow
AES	Advanced Encryption Standard
AM-HT	Armenian financial messaging format, which bases upon the Swift MT Standard
AML	Anti-Money Laundering
AMD	Armenian Dram
API	Application Programming Interface
ArCa	Armenian Card
BIC	Bank Identifier Code
BIS	Bank for International Settlements
CBA	Central Bank of Armenia
CBPR+	Cross-Border Payments and Reporting Plus
CDA	Central Depository of Armenia
CFT	Countering the Financing of Terrorism
CI/CD	Continuous Integration / Continuous Deployment
CIPS	Cross-Border Interbank Payment System
CPU	Central Processing Unit
CSV	Comma-Separated Values
DR	Disaster Recovery
EBRD	European Bank for Reconstruction and Development
ELK	Elasticsearch, Logstash, Kibana
FMI	Financial Market Infrastructure
GDPR	General Data Protection Regulation
GPI	Global Payments Innovation
GSASS	Government Securities Accounting and Settlement System
HVPS+	High-Value Payment System Plus
IEC	International Electrotechnical Commission
IMF	International Monetary Fund
ISO	International Organization for Standardization
ISO-AM	ISO 20022 Armenia
IT	Information Technology
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LEI	Legal Entity Identifier
MFA	Multi-Factor Authentication



Acronyms	Full Names
NBFIs	Non-Bank Financial Institutions
NDA	Non-Disclosure Agreement
NFR	Non-Functional Requirements
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
PFMI	Principles for Financial Market Infrastructures
RA	Republic of Armenia
RBAC	Role-Based Access Control
REoI	Request for Expression of Interest
RFP	Request for Proposal
RPO	Recovery Point Objective
RT0	Recovery Time Objective
RTGS	Real-Time Gross Settlement
RUB	Russian Ruble
SFTP	Secure File Transfer Protocol
SEPA	Single Euro Payments Area
SLA	Service-Level Agreement
SME	Small and Medium-Sized Enterprises
SOC	System and Organization Controls
SPFS	System for Transfer of Financial Messages
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TLS	Transport Layer Security