Request for expressions of interest

CONSULTING SERVICES - Adaptive maintenance for the existing CGF'S Information System

REPUBLIC OF MOLDOVA
MICRO, SMALL AND MEDIUM-SIZED ENTERPRISES COMPETITIVENESS PROJECT
Sector: General industry and trade sector
IDA Credit No. 71740
IBRD Loan No. 94230
Project ID No. P177895
Reference No. MD-CEP-474691-CS-CQS

The Republic of Moldova has received financing from the World Bank toward the cost of the Micro, Small and Medium-Sized Enterprise Competitiveness Project (MSME) and intends to apply part of the proceeds for consulting services.

The consulting services ("the Services") comprise adaptive maintenance for the existing CGF Information System to ensure full compliance with applicable national requirements regarding interoperability architecture, cybersecurity, personal data protection, and digital governance established by competent authorities, including the Information Technology and Cyber Security Service (STISC). The system must utilize modern technologies and remain compatible with MCloud.

The assignment is expected to be completed within 32 weeks from contract signing. Additionally, the scope includes a 2-month stabilization period following deployment, a 3-month warranty and extended maintenance period following stabilization, and a 6-month extended maintenance period following the expiration of the warranty.

The Terms of Reference (TOR) for the assignment is attached to this request for expressions of interest.

The Project Implementation Unit of the MSME Competitiveness Project now invites eligible consulting firms ("Consultants") to indicate their interest in providing the Services. Interested Consultants should provide information demonstrating that they have the required qualifications and relevant experience to perform the Services (required qualifications and experience of the firm, but not individual experts' bio data).

This assignment requires a consultant, which shall be a consulting firm or a consortium of consulting firms, with proven experience in the field of the assignment, that meets the following minimum criteria:

- The company shall be a legally registered entity with demonstrated experience of minimum 7 years in software development, modernization and maintenance of enterprise information systems.
- The company has demonstrated successful completion of at least 3 information systems of comparable complexity development or modernization assignments during the last 5 years.
- The company has experience with Government information systems integrated with Government interoperability platforms, including in financial-sector, banking, lending or risk-management information system.
- The company has technical staff with extensive knowledge and experience with implementation of software projects based on Laravel Framework; PHP development; SQL; JavaScript, Ext JS and enterprise front-end frameworks; REST APIs and web services.

- The Company shall have successfully completed at least one assignment involving financial guarantee systems, banking systems, lending platforms, or comparable financial-sector information systems.

The Consultant shall ensure that the proposed team includes qualified experts covering the following roles:

- Team Leader / Project Manager – with academic background in Information Technologies, Computer Science, or related field.
- Business Analyst – specialized in business process analysis and requirements engineering.
- System Architect – with expertise in enterprise system architecture and integration.
- Senior Back-End Developer – proficient in PHP and Laravel for large-scale information systems.
- Front-End Developer – skilled in JavaScript-based frameworks for user interface development.
- Database Specialist – competent in database administration and optimization.
- QA and Testing Specialist – specialized in software quality assurance and testing.
- Cybersecurity Specialist – responsible for ensuring system security and compliance.

The attention of interested Consultants is drawn to Section III, paragraphs, 3.14, 3.16, and 3.17 of the World Bank's "Procurement Regulations for IPF Borrowers" November 2020 ("Procurement Regulations"), setting forth the World Bank's policy on conflict of interest. A Consultant will be selected in accordance with the „Consultant's Qualification-based Selection" method set out in the Procurement Regulations.

Consultants may associate with other firms to enhance their qualifications; but should indicate clearly whether the association is in the form of a joint venture and/or a sub-consultancy. In the case of a joint venture, all the partners in the joint venture shall be jointly and severally liable for the entire contract, if selected.

The Expression of Interest shall clearly state the name of the Consultant (individual Firm, Joint Venture or sub-consultancy). The Consultant shall provide relevant references (assignment name, Client, time frame, the role of the firm (main Consultant/Partner in JV/sub-consultant, contract amount, tasks performed etc.) to confirm its experience and qualifications.

Further information can be obtained at the address below during office hours.

Expressions of interest must be delivered in a written form to the address below (in person, or by mail, or by e-mail) by **August 04, 2026**, COB.

Project Implementation Unit of the MSME Competitiveness Project
180, Stefan cel Mare Ave., office 815, MD-2004, Chisinau, Republic of Moldova
Tel: + 373 22 296-723
e-mail: piu@mded.gov.md
web: www.uipac.md

E-mail for submission of the **clarifications: piu@mded.gov.md**

E-mail for submission of the **EoIs: procurementmgf@gmail.com**

ONLY THE NOTIFICATION OF EOI SUBMISSION MUST BE SENT TO PIU@MDED.GOV.MD

TERMS OF REFERENCE
ADAPTIVE MAINTENANCE FOR THE EXISTING CGF'S INFORMATION SYSTEM

A. Background

The Government of the Republic of Moldova (GoM), with the support of the World Bank, is implementing the MSME Competitiveness Project aimed at improving access to finance, enhancing export competitiveness, and strengthening institutional capacities supporting micro, small and medium-sized enterprises (MSMEs).
Under Component 2 – Access to Finance, the Project supports the Credit Guarantee Facility (CGF) managed by the Organization for the Development of Entrepreneurship (ODA). The CGF facilitates MSME access to finance by providing financial guarantees to participating financial institutions.

To support operationalization and digitalization of guarantee processes, the Information System for Credit Guarantee Facility (GMS) was developed and deployed. The system supports the full lifecycle management of financial guarantees, including application, assessment, approval, issuance, monitoring, reporting, modification, and execution of guarantees.
The GMS is integrated with Government digital infrastructure and interoperability services, including MPass, MSign, MConnect, MCloud, and other public information systems and registries. The system supports multiple stakeholders, including ODA personnel, participating financial institutions, public authorities, and guarantee beneficiaries.
The GMS operates in accordance with the Government Decision No. 787 of 25 October 2023, approving the Concept of the Information System for Credit Guarantee Facility and related regulatory framework governing its operation, interoperability, data exchange, administration, and information security requirements. The system forms part of the national digital government ecosystem and shall comply with applicable Government interoperability architecture, cybersecurity, personal data protection, and digital governance requirements established by the competent authorities, including the Information Technology and Cyber Security Service (STISC).

The current architecture of the GMS system is based on:

- Back-end technologies: Laravel PHP framework
- Front-end technologies: JavaScript and Ext JS framework

Information system architecture

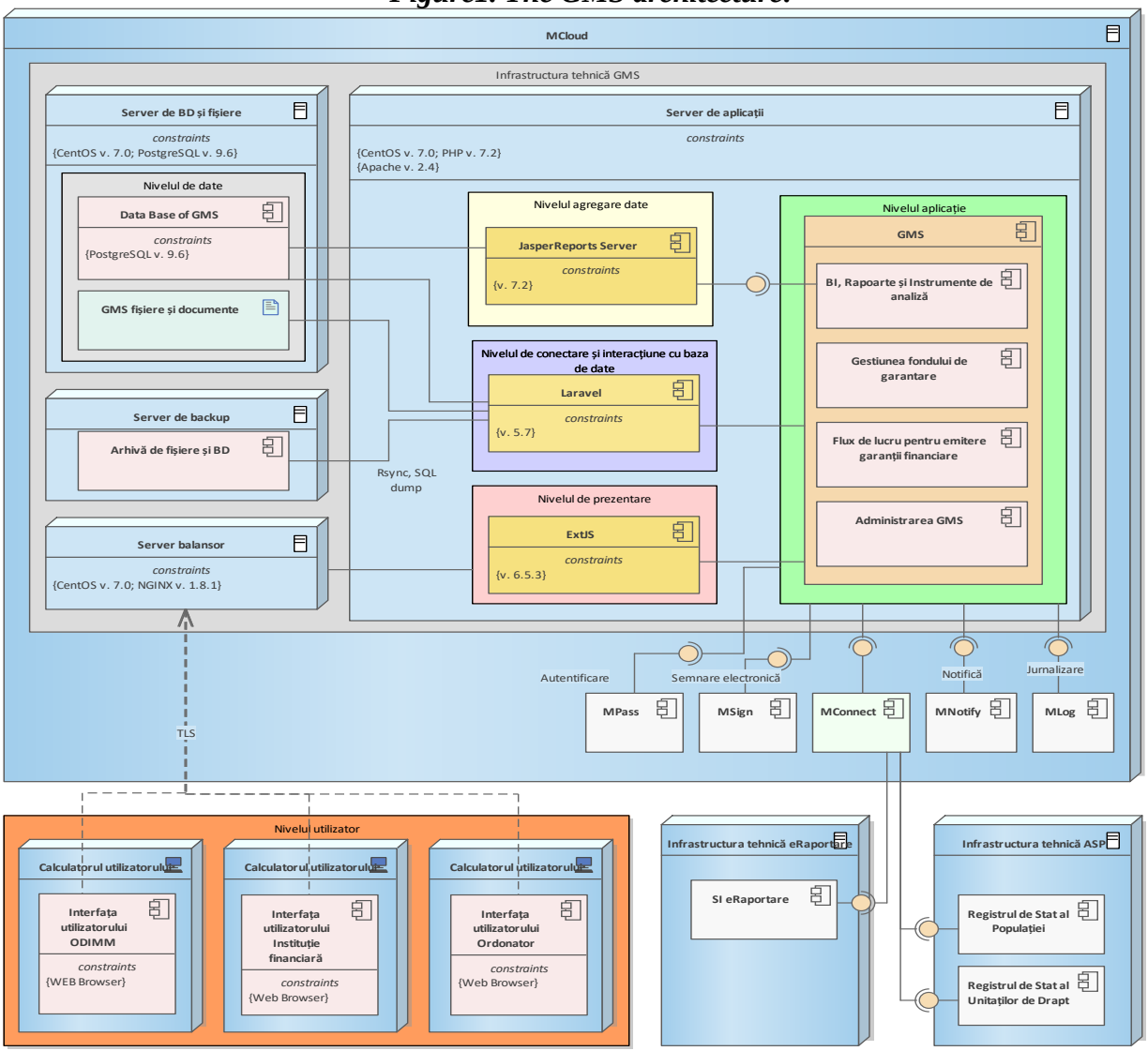
Physical architecture of the information system

The GMS information system will be based on modern technologies and compatible with MCloud. The infrastructure required to host the solution consists of a server with secured access to the GMS application database. GMS will be accessed from the outside via an external IP at www.gms.ODA.md.
In order to ensure an adequate level of information security, the delivered IT solution must allow the creation of secure connections between client stations and the application server to ensure the safety of the sent information (via VPN channels and TLS/SSL sessions).
The IT solution is to be developed based on the Internet/Intranet technologies suitable for the moment. The interaction of all actors and nodes of the IT subsystem is shown in Figure 1.
As shown in Figure 1, the resource cooperation solution to ensure GMS functionality consists of 4 distinct node categories:

- **MCloud** - the ICT infrastructure of the common government technology platform that forms the government cloud (MCloud) where MPass, MSign, MLog and MConnect platform service is hosted with which GMS must be integrated. The inclusion in the architecture of the MConnect service bus allows integration with the services of other IT systems hosted also outside MCloud (State Register of Law Units, State Register of Population and Financial Data Bank reported annually by enterprises).
- **Data Center of the Public Services Agency** - the ICT infrastructure of the Public Services Agency where the RSUD and RSP with which the GMS is to be integrated is hosted. The interaction will be carried out through the MConnect interoperability platform.
- GMS will retrieve financial data reported by enterprises from MConnect interoperability platform.

From a functional point of view, 4 main categories of system users can be distinguished: Authorised users from ODA, authorised users from financial institutions, authorised users with the role of Authorising Officer, authorized users from the SME side. Regardless of the level of user access, all user connections to the GMS will be made through secure connections (via the SSL/TLS protocol).

Figure1. The GMS architecture.



In order to ensure optimal functionality, GMS will consume the following categories of interfaces provided to third-party IT systems:

1. User **Authentication Service that** interacts with the governmental MPass platform service for the purpose of implementing user authentication procedures by means of electronic signature or mobile signature;

2. Electronic **signature service that** interacts with the governmental MSign platform service for the purpose of implementing electronic signature procedures for documents managed by GMS;
3. **Notification** Service interacting governmental notification MNotify for the transmission of notifications within information systems owned by ministries, administrative authorities and organizational structures within their remit, as well as other public institutions providing public services.
4. The **Logging** Service interacting with the governmental MLog notification for recording and monitoring data exchanges and recording types of critical events in the information system, in order to ensure the appropriate security regime, in accordance with the legislation on the protection of personal data and other special data regimes.
5. Service **receive legal entities data** interacting with the State Register of Law Units managed by the Public Services Agency for the purpose of taking over the registration data of entities (State aid beneficiaries) managed by the GMS.
6. Service **receive individuals' data** interacting with the State Population Register managed by the Public Services Agency for the purpose of taking over the registration data of individuals (State aid beneficiaries or business leaders and founders) managed by GMS.
7. Service **receive financial data** interacting with the Mconnect from where GMS will retrieve the necessary financial data that are reported annually by businesses.

Logical architecture of the information system

GMS will provide a WEB interface accessible via a widely used Internet Explorer (Microsoft Edge/Microsoft Internet Explorer, Mozilla FireFox, Opera, Google Chrome or Safari). From a functional point of view, a reliable and scalable solution will be developed both in the case of an increase in the number of competing users or in the case of an increase in the volume of information managed by it based on an MVC architecture.

. As GMS is not an isolated IT solution, but will interact with external IT systems (RSP, RSUD, FSC, etc.), the developed IT solution will provide support for integration with other IT subsystems (SOA architecture).

The architecture model used is the Layer-based design model (layers). This architecture provides a way to break down the computer system into more manageable software components and narrow down inter-system dependencies in order to design a solution that is easier to sustain. An important feature of this design model are the directed dependencies that exist between different layers of the system.

This approach isolates and organizes different system responsibilities into a hierarchical structure consisting of the following layers:

- **Presentation Layer (UI)** - this top-layer (level) provides support for interactions between actors or users of the system;
- **Business Logic Layer** - this middle-layer provides support for applications specific to business processes, such as the application and execution of business rules and integrity;
- **Data Access Layer** - this bottom-layer, provides support to access data and persistence using the relational database.

As shown in Figure 1, GMS follows an MVC or Model-View-Controller architecture type.

Due to the chosen architecture, the continuous development of the information system as a result of the division of the information system on different levels relatively independent from a functional point of view will be easy in the future.

Thus, the presentation level (which corresponds to the view part of the application) does not need to know the mechanisms for implementing the connections to the database and the data processing algorithms, but

exposes a series of templates that the other levels must use in order to correctly present the interface and the data.
On the other hand, the splitting of the data application creates relative independence from the technology used for data storage and management (database management system), with the result that it is possible to modify the database management system if necessary without affecting the application level.

Platform and tools used
The GMS information system will be installed and will operate on the MCloud Government Platform. According to this, GMS must ensure compatibility with MCloud technologies.

Figure2. Diagram of the technical infrastructure of the GMS information system.

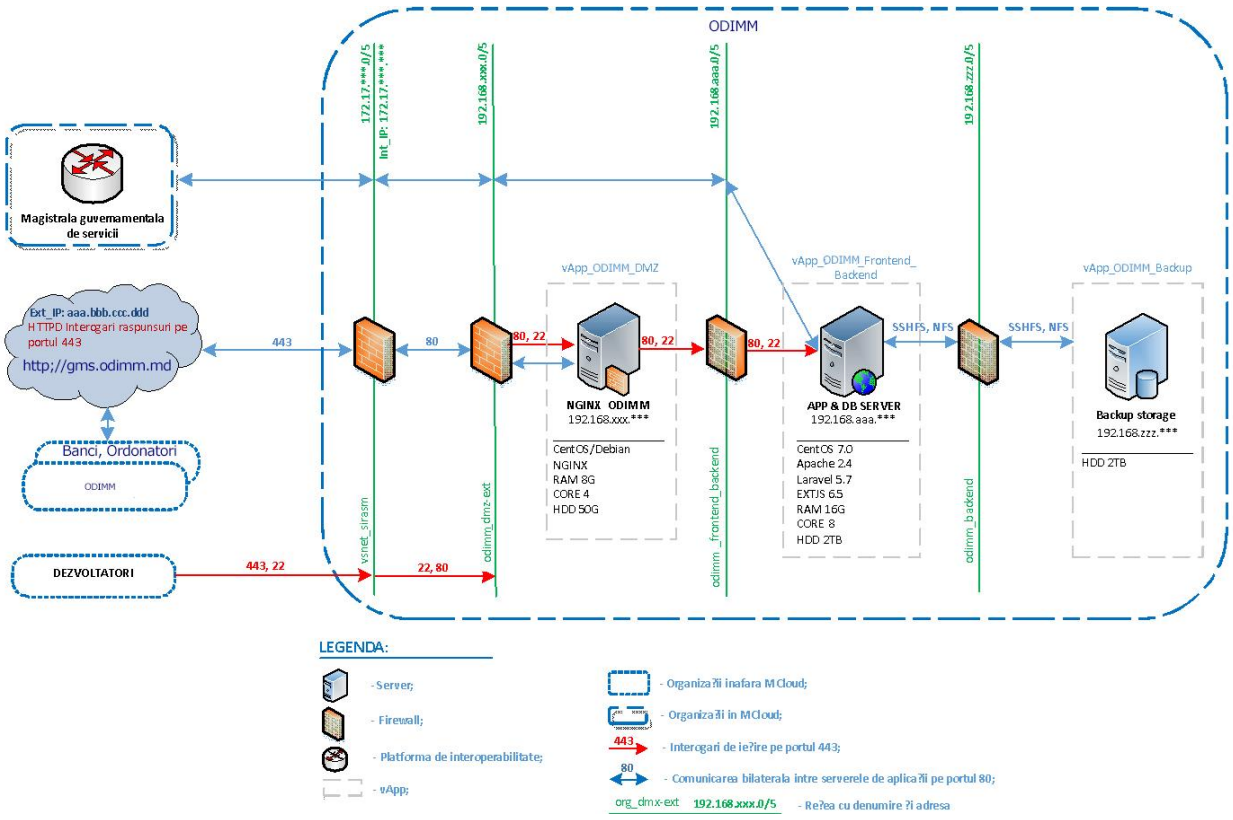


Figure 3 shows the diagram of the technical infrastructure required to set up on the MCloud government platform. ODA must negotiate with the E-Governance Agency the conditions for obtaining access to the MConnect interoperability service.

Operating system. ***Linux***.
Web server. as a Web server for *GMS* it is used ***Apache HTTP Server***.
Database SGBD. As a Database Management System at the elaboration of *GMS* was chosen one of the most performant and advanced open source IT solutions at the moment: ***PostgreSQL***.
Web programming language. ***PHP programming language***.
Technological Development Platform. As a technology platform is used: ***Laravel ,*** which allows the implementation of an *architectural model of MVC* type, requires minimal operating resources while ensuring an increased performance considered to be the standard for WEB solutions integrated with PHP,

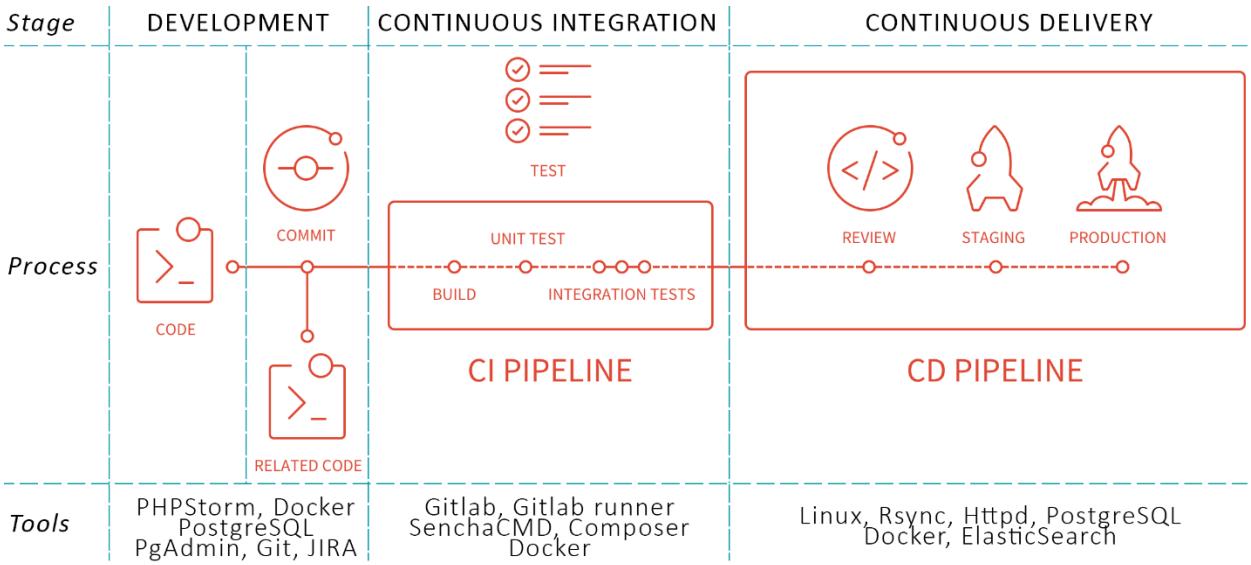
is well documented and easy to study, provides a wide set of libraries and modules that allow to reduce the development time of the program code.

User Interface Development Platform. As a GMS user interface development solution, the use of the Java Script ***EXT JS*** library is used, enabling the implementation of an *MVC* architectural model, requiring minimal operating resources while ensuring increased ergonomics and portability on all software platforms.

For the development, testing and implementation in production of the *GMS* information system, 3 working environments will be configured and used:

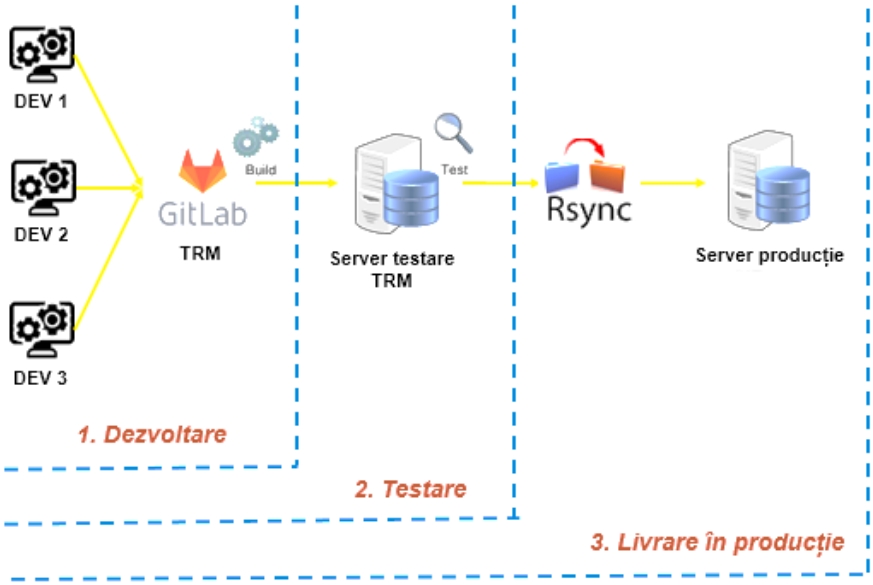
- **Development Environment** – is the working environment used by programmers to develop the IT solution. This environment will be configured and maintained by the *Developer*. In order to facilitate the process of continuous delivery of the IT solution, the development will be done on virtual environments with distributable configurations based on Docker technology.
- **Test environment** – is the environment where the product will arrive after continuous integration and automated testing procedures. This environment will be made available by the *Developer* for the purpose of testing the functionalities of the IT system before delivery to the production environment.
- **Production environment –** is the production environment of the information system. This environment will be provided by the *Beneficiary*. *The beneficiary shall* ensure the maintenance of the server infrastructure of the production environment and all accesses and access permissions at server level necessary for the normal operation of the *GMS* information system.

Figure3. The architecture of integration and continuous delivery of the GMS information system.



All configuration and development work will be carried out on the Development Environment on the *Developer's* platform. Also on the *Developer side will* be installed the GIT repositorie server for storage, versioning and code management. Once a stable version (stage) has been completed, the system shall be run on the *Developer Test Environment* . *The beneficiary will* test the current version (current phase) and then draw up a test report.

Figure 5. The steps in the process of integration and continuous delivery of the IT solution.



In the case of adjustments, the system will be tested repeatedly and only after final acceptance will it be delivered to the Production Environment. All code manipulations are performed exclusively by GIT commands. Thus, for each version will be made ChekPoints or separate Branches. The beneficiary will have a separate branch called production. On the Production Environment, after cloning the system, only the PULL function will be used.

Given the evolving operational, regulatory, technological, and cybersecurity requirements, the GMS requires continuous: corrective, adaptive and preventive maintenance; modernization and source code upgrades; development of new modules and functionalities; enhancement of interoperability mechanisms; and optimization and refactoring of the existing codebase.

ODA has identified the need for substantial system upgrades related to:

- implementation of new guarantee products;
- portfolio guarantee schemes;
- existing state guarantee products;
- risk management and internal control processes;
- provisioning calculations;
- state aid calculations;
- automated reporting and integrations with banking systems;
- management of related-party/group exposures.

In this context, the Project Implementation Unit (PIU) intends to contract a specialized IT company to provide upgrading, adaptive maintenance, modernization, technical support, and evolutionary development services for the GMS.

B. Scope of Work

The Company shall implement, configure, test, document and deploy the functional enhancements described below and ensure their seamless integration with the existing GMS architecture:

1. Automated Data Collection and Interoperability. Adjust and expand automated collection of information from public databases and registries, including through MConnect, ASP, BNS, RSUD, State Tax Service and other relevant information systems, including of related-party/group exposures.
2. New Forms and Guarantee Product Templates. Develop and adjust application forms, workflows, templates and supporting documents required for existing and future guarantee products administered by ODA.
3. Workflow Modernization. Adjust approval, modification, monitoring, execution and reporting workflows in accordance with the Operational Manual, internal procedures and future operational requirements of ODA.
4. Related Parties Registry and Group Exposure Monitoring. Create and maintain a registry of persons and entities related to guarantee beneficiaries and applicants and implement automated group exposure verification mechanisms.
5. Risk Management and Internal Control Module. Develop dedicated interfaces, workflows and user roles for risk management specialists, including risk opinions, exposure verification, concentration monitoring and internal control procedures.
6. Exposure and Capital Management Functionality. Implement functionality for monitoring and management of guarantee exposure limits by creditor, beneficiary, affiliated group and economic activity sector, including dashboards and automated alerts.
7. Provisioning Module. Develop automated provisioning calculation mechanisms for issued guarantees, including reporting, monitoring and audit trail functionalities.
8. State Aid Management Module. Develop automated state aid calculation mechanisms, beneficiary notification functionality and state aid reporting tools in accordance with applicable legislation and ODA procedures, including the integration with the State Aid Registry.
9. Banking Integration and Automated Reporting. Enhance integration with participating financial institutions and develop automated collection, validation and processing of creditor reports and portfolio information.
10. “Prima Casă” State Guarantee Management. Develop dedicated interfaces, user roles and workflows for administration of Prima Casă state guarantees.
11. “Prima Casă” Approval and Document Management Workflows. Develop approval, issuance, modification, monitoring, execution and document generation workflows related to “Prima Casă” guarantees, including reporting and audit functionalities.
12. Migrate the existing "Prima Casă" database into GMS and integrate it with the implemented workflows.
13. Additional minor Functional Requirements for Modernization of the GMS upon ODA’ request**.**

14. Banking delegation mechanism. Develop the mechanism for the temporary delegation of responsibilities within the platform for the bank directors, appointing managers to multiple branches with a clearly defined delegation period.
15. Consolidating multiple guarantee applications. Develop dedicated workflow for enabling the grouping of multiple submitted guarantee applications into a single analysis and approval workflow, with the generation of a single consolidated document covering all grouped applications.
16. Configurable timer for conditionalities. Implement a configurable deadline for the actions required under the guarantee approval decision, including notifications and marking whether each required condition has been fulfilled or not.
17. ITCSS software version compliance. Updating the GMS software to the latest available version, in correspondence with the ICTSS requirements, and verifying the system's integrity, functionality, and operational readiness following the update.

Prior and during the development of the upgrades the Developer is expected to perform for each upgrade the following tasks:

- Provide business analysis and prepare/update technical documentation;
- Provide test cases and test reports;
- User acceptance test report (UATs);
- Update user and admin guides (if needed);
- Deploy the updates of changes to production environment (with the Client permission);

Testing requirements

After finalization of the services, new adjusted software should be tested by Company to confirm the correspondence to the quality assurance requirements.

Training and training materials

The Company MUST provide training for 2 persons from among ODA staff with the role System Administrator with a minimum 24 hours program.

The Company must provide training for 2 trainers of GMS from among ODA staff with a minimum 24 hours program

The Company must provide advice to the financial institutions in GMS-APIs implementation.

The Company must deliver all training materials.

The Company must develop a guide for ODA and banks regarding the use of the system functionalities.

All trainings, including training materials will be developed and conducted in Romanian language.

Service Level Agreement (SLA)

The Company shall ensure the following minimum service levels during the stabilization, warranty and extended maintenance periods:

Incident Priority	Description	Initial Response Time	Target Resolution Time
Critical	Complete or significant interruption of the GMS preventing guarantee processing or affecting system availability, security or integrity	**30 minutes**	**8 business hours**
High	Major functionality unavailable or severe degradation	**2 business hours**	**24 business**

	affecting business operations without a complete system outage		**hours**
Medium	Functional defect affecting a limited number of users or non-critical business processes	**1 business day**	**5 business days**
Low	Minor defects, cosmetic issues, enhancement requests or other non-critical issues	**3 business days**	As mutually agreed through the approved work plan

The Company shall maintain a ticketing mechanism for registering, tracking and resolving all reported incidents. Each ticket shall be assigned a unique reference number and its status shall remain available to ODA throughout its lifecycle. Assigned ODA staff should be one of signing off on closing the ticket.

Where an incident cannot be resolved within the target resolution time, the Company shall promptly notify ODA, explain the reasons for the delay, propose interim mitigation measures, and agree on a revised resolution schedule.

End-users support. The end-user shall report all technical issues that could occur through a ticketing mechanism, E-mail or instant message.

Technical assistance. Technical assistance will be provided by the qualified technical personnel of the Company. The composition of the team and its modification will be agreed by parties. The technicians will investigate and solve reported technical deficiencies. The manager will serve as a contact point and for forwarding of requests. The Company shall ensure support to document the technical issues and their traceability for the Beneficiary.

Post-warranty maintenance services. The Company must ensure its capacity to provide technical support beyond the warranty period. The extended warranty period is 6 months. The conditions and volume of works in the extended maintenance period should be included in the financial offer as part of the optional costs.

Documentation requirements

The Company must deliver updated Guidelines in Romanian language for all categories of users (at least: user guideline and administration guideline)

The Company must update and deliver the interactive guidance materials in Romanian language included in the GMS user interface.

The Company must update and deliver training documentation for all type of GMS users.

The Company must update and deliver the system installation and configuration guide (which includes at least the code compilation, application installation, CI/CD means, hardware and software requirements, platform description and configuration, application configuration, disaster recovery procedures).

Technical documentation of the information system

The Company must update and deliver the technical project (SRS and SDD) according the performed adjustments and changes to the delivered software.

The Company must update (if needed) and deliver the system architecture documentation with the description of models in UML language, which will include an enough level of details of the architecture in several sections.

The Company must update and deliver the documentation of APIs exposed for integration with external IT Systems.

The Company must deliver fully documented source code for applications and components changed or developed during the project activities.

The Company must deliver Libraries and special instruments necessary for compilation of GMS components.

The Company must prove the possibility to compile the source code.

The Company must deliver the final product packed for easy installation in the proposed technological environment.

The Company must deliver the Continuous Integration/Continuous Delivery means for GMS.

C. Schedule of Implementation of Services / Tentative Work Plan

The implementation schedule below is indicative and may be refined following the inception phase, business analysis, and validation of detailed requirements by ODA.

Stage	Deadline	Main Activities and Deliverables
Stage I – Inception and Business Analysis	4 weeks from contract signature	Review existing source code, database structure, integrations and technical architecture. Conduct detailed business analysis. Validate requirements with ODA. Update SRS, SDD, UML models and technical architecture documentation. Prepare detailed implementation roadmap and backlog of functionalities.
Stage II – Core Business Process Modernization	8 weeks from contract signature	Combination of Application and Guarantee Request. Dual-signature functionality. Product eligibility engine. Simplified Committee workflows. User management enhancements. Financial limits management. Guarantee file management. Dedicated workflow for consolidating multiple guarantee applications. Credit classification and provisioning setup. Timer for guarantee conditionalities.
Stage III – Risk Management and Internal Control	12 weeks from contract signature	Development of Risk Management Module. Risk opinions. Exposure monitoring. Concentration controls. Early warning indicators. Internal control workflows. Related Parties Registry. Group Exposure Monitoring. Exposure dashboards and automated alerts.
Stage IV – Guarantee Operations and Compliance Modules	16 weeks from contract signature	Provisioning Module. State Aid Management Module. Collateral substitution workflow. Recovery and enforcement workflow. Event journaling and historical reporting functionality. Automated state aid calculations and notifications.
Stage V – Prima Casă	20 weeks from contract signature	Development of Prima Casă State Guarantee Module. Approval and document management workflows. Portfolio monitoring and reporting. Automated exposure tracking. Claim management functionality.
Stage VI – Banking Integration and Interoperability	24 weeks from contract signature	Banking systems integration. Automated creditor reporting. API development. MConnect integrations. Data retrieval from ASP, State Tax Service, BNS, RSUD and other public registries. Synchronization services and automated validations.
Stage VII – Reporting, Analytics and Dashboards	28 weeks from contract signature	Development of operational dashboards. Risk dashboards. Portfolio monitoring reports. State aid reports. Exposure reports. Regulatory reporting tools. Analytical and statistical reporting enhancements.
Stage VIII – Testing and Acceptance	32 weeks from contract signature	Functional testing. Integration testing. Performance testing. Security testing. User Acceptance Testing (UAT). Correction of defects. Preparation of final release package.

Stage IX – Training and Deployment	During the implementation upon request	Training of system administrators. Training of trainers. Delivery of user manuals and technical documentation. Production deployment. Final acceptance.
Stage X – Stabilization Period	2 months following deployment	Production support. Bug fixing. Performance tuning. Incident management. Monitoring and optimization. Monthly maintenance reports.
Stage XI – Warranty and Extended Maintenance	Minimum 3 months following stabilization	Warranty support, adaptive maintenance, technical assistance, security updates, interoperability support and post-warranty maintenance services.
Stage XII – Extended Maintenance Services	6 months following completion of the Warranty Period (if exercised by ODA)	Adaptive maintenance, technical support, implementation of minor enhancements, interoperability adjustments and operational assistance under the Service Level Agreement (SLA).

The implementation sequence presented above reflects the priorities identified by ODA at the time of preparation of these Terms of Reference. ODA and PIU reserve the right to reprioritize, defer, replace, supplement or expand individual functionalities during implementation, subject to operational needs, regulatory developments and approval of corresponding change requests.

D. Reporting Arrangements

The Consultant shall report to the Organization for the Development of Entrepreneurship (ODA) and the Project Implementation Unit (PIU).

All deliverables shall be submitted in Romanian language in editable electronic format (MS Word, Excel, Visio, PDF and source files where applicable).

The Consultant shall prepare and submit the following deliverables:

D.1. Inception Phase Deliverables

Within four (4) weeks from contract signature, the Consultant shall submit:

- Inception Report;
- Detailed Work Plan and Implementation Schedule;
- Business Analysis Report;
- Functional Requirements Specification;
- Updated System Architecture Documentation;
- Legacy Issues and Non-Conformities Register

System Requirements Specification Document (SRS) and Software Design Document (SDD) will be subject of permanent update throughout the whole implementation period. Final version of the SRS and SDD will be submitted as part of the final deliverable’s package foreseen under D.6.

D.2. Development Deliverables

For each module and functionality developed, the Consultant shall submit:

- Technical Design Documentation;
- Source Code and Configuration Files;
- Test Cases and Test Results;
- Deployment Documentation;
- Updated User Manuals;
- Updated Administrator Manuals;
- Updated API Documentation (where applicable).

D.3. Testing Deliverables

The Consultant shall prepare and submit:

- Unit Testing Report;
- Integration Testing Report;
- Performance Testing Report;
- Security Testing Report;
- User Acceptance Testing (UAT) Report;
- Defect Resolution Report.

D.4. Training Deliverables

The Consultant shall submit:

- Training Agenda;
- Training Materials;
- Training Attendance Records;
- Training Completion Report.

D.5. Operational Support Deliverables

During stabilization and warranty periods, the Consultant shall submit monthly:

- Maintenance Report;
- Incident Management Report;
- Service Level Performance Report;
- Corrective Actions Report;
- Change Request Register;
- Security and Vulnerability Management Report.

D.6. Final Deliverables

At completion of the assignment, the Consultant shall submit:

- Final Project Report;
- Final Updated SRS and SDD;
- Complete Source Code Repository;
- Deployment Package;
- System Architecture Documentation;
- Disaster Recovery Documentation;
- Knowledge Transfer Report;

- Final Acceptance Package.
- All deliverables shall be subject to review and approval by ODA.

E. Qualification Requirements

The Company shall demonstrate proven experience following the requirements below and shall designate and ensure the availability of a team of qualified experts:

- The company shall be a legally registered entity with demonstrated experience of minimum 7 years in software development, modernization and maintenance of enterprise information systems.
- The company has demonstrated successful completion of at least 3 information systems of comparable complexity development or modernization assignments during the last 5 years.
- The company has experience with Government information systems integrated with Government interoperability platforms, including in financial-sector, banking, lending or risk-management information system.
- The company has technical staff with extensive knowledge and experience with implementation of software projects based on Laravel Framework; PHP development; SQL; JavaScript, Ext JS and enterprise front-end frameworks; REST APIs and web services.
- The Company shall have successfully completed at least one assignment involving financial guarantee systems, banking systems, lending platforms, or comparable financial-sector information systems.

The Consultant shall ensure that the proposed team includes qualified experts covering the following roles:

- Team Leader / Project Manager – with academic background in Information Technologies, Computer Science, or related field.
- Business Analyst – specialized in business process analysis and requirements engineering.
- System Architect – with expertise in enterprise system architecture and integration.
- Senior Back-End Developer – proficient in PHP and Laravel for large-scale information systems.
- Front-End Developer – skilled in JavaScript-based frameworks for user interface development.
- Database Specialist – competent in database administration and optimization.
- QA and Testing Specialist – specialized in software quality assurance and testing.
- Cybersecurity Specialist – responsible for ensuring system security and compliance.

Availability of Resources

The Consultant shall ensure availability of qualified personnel throughout the implementation period and shall maintain the proposed key experts unless otherwise approved by ODA and PIU.

Replacement of key experts shall be subject to prior approval, and the replacement expert shall possess qualifications and experience equal to or better than those originally proposed.