Request For Expressions of Interest - Consultant’s Qualifications Based Selection (CQS): Audit services of the information technology infrastructure and of the level of cyber security within the Public Institution Real Estate Cadastre, ref Nr. MD-PSA-4990

Name of Project	***Land Registration and Property Valuation Project***
Loan No/Credit No/ Grant Number	**6306-MD**
Assignment Title	**Audit services of the information technology infrastructure and of the level of cyber security within the Public Institution Real Estate Cadastre**
Procurement Plan Ref Number	**MD-PSA-499049-CS-CQS**
Country of Delivery	**Republic of Moldova**
Date	**23.06.2025**

REQUEST FOR EXPRESSIONS OF INTEREST
CONSULTANT’S QUALIFICATIONS BASED SELECTION
(CQS)

The Government of Republic of Moldova has received financing from the World Bank toward the cost of the Land Registration and Property Valuation Project and intends to apply part of the proceeds for the following consulting services.

The Consultant will provide audit services of the information technology (IT) infrastructure and of the level of cyber security within the ***Public Institution Real Estate Cadastre***, in accordance with the Terms of Reference specified in this document.

1. THE MAIN OBJECTIVES OF THE AUDIT ARE:

a. Assessment of IT infrastructure and the current state of cyber security within the PI REC.
b. Identifying gaps, inefficiencies and vulnerabilities within IT infrastructure and cyber security.
c. Determining channels and technical solutions to ensure the interoperability of information systems managed by PI REC with other government information systems.
d. Providing actionable recommendations for strengthening IT infrastructure and cyber security measures.
e. Developing an action plan to implement the recommendations of the IT infrastructure audit and the level of cyber security, as well as a plan to address major risks. When developing recommendations and an action plan to improve the IT infrastructure and increase cyber

resilience, the Consultant will take into account the development prospects of the PI REC, ongoing projects at the time of the audit, as well as the transition of the IT infrastructure to a new architecture.

2. SCOPE OF SERVICES AND TASKS

The consultant will ensure the fulfillment of the following tasks:

2.1. **Audit of the IT infrastructure of PI REC**

a. Inventory evaluation:
   - Analysis of hardware assets, software, software licenses, and application programs used for cadastral and telecommunications information systems.
   NOTE: In October 2024, IP CBI conducted its annual inventory of all owned assets, with updated data reflected in the accounting records.
   Assessment of server infrastructure, storage systems, and network equipment.
b. Network architecture assessment:
   - Network topology and configuration evaluation;
   - Data flow analysis, bandwidth usage and redundancy mechanisms;
   - Identifying limitations or bottlenecks in the network and servers;
   - Evaluation of firewall, intrusion prevention systems (IPS) and intrusion detection systems (IDS);
   - Evaluation of communication protocols used in the network to ensure data transfer security.
c. System performance and optimization:
   - Evaluating server performance, storage capacity and resource utilization;
   - Assessing scalability and future growth needs, including to ensure interoperability with other government systems.
   - Identifying areas that need improvement.
d. Evaluation of the degree of interoperability between systems:
   - Checking compatibility and synchronization between IS "REC" modules;
   - Analysis of the interoperability of information subsystems managed by PI REC with other platforms and external applications;
   - Examination of protocols and data formats used for exchanging information between systems.
e. IT Operations and Processes:
   - Review of IT management practices, including change, incident and asset management.
   - Evaluation of IT systems maintenance procedures and response times.
f. Business continuity and disaster recovery:
   - Reviewing backup procedures and disaster recovery plans;
   - Validation of business continuity plans and testing of recovery processes;
   - Assessing data restoration capabilities following critical incidents.
g. cloud virtualization systems:
   - Security analysis of virtual machines and virtualized infrastructure;
   - Verifying the segmentation of cloud resources and the security mechanisms applied to them;
   - Assessing the integrity and security of access to cloud resources.

2.2. **Cyber Security Audit:**

a. Risk assessment and threat analysis:
   - Identifying potential cyber security threats and risks;
   - Evaluation of threat detection and response mechanisms;
   - Review of procedures and regulations for managing detected information security incidents.
b. Security and compliance policies:
   - Review of cyber security policies, standards and procedures;
   - Assessing compliance with national and international cyber security regulations.
c. Vulnerability assessment:
   - Performing internal and external vulnerability scans;
   - Identifying misconfigurations or improper configurations that may pose security risks.
d. Testing for unauthorized access:
   - Simulating real cyber-attacks to assess the defense of PI REC's IT infrastructure;
   - Identifying exploitable vulnerabilities and their potential impact.
e. Penetration testing of IT infrastructure using the PENTEST (White Box) method.
f. Access control and identity management:
   - Review of access controls and authentication mechanisms used.
   - Evaluation of password policies and implementation of multi-factor authentication;
   - Analysis of remote access security to IT infrastructure.
g. Incident response and monitoring:
   - Evaluation of the incident response plan and procedures;
   - Review of monitoring tools and logging mechanisms;
   - Evaluation of plans and procedures for handling incidents that occurred prior to the audit;
   - Compliance assessment regarding CERT-Gov notification in case of cyber incidents, according to legal requirements.
h. Awareness and Training:
   - Assessment of staff awareness regarding cyber risks, security best practices, and the protection of personal and sensitive data;
   - Analysis of planned training programs, including the frequency, relevance, and effectiveness of the conducted sessions;
   - Identification of gaps in staff knowledge and competencies;
   - Development of recommendations for strengthening the security culture.
   - Evaluation of staff awareness and training programs in the fields of IT technologies and cyber security;
   - Identifying gaps in staff knowledge and skills.
i. Evaluating updates and patching:
   - Analysis of the efficiency of software and firmware update procedures;
   - Identifying potential delays in applying critical patches.
j. Evaluation of security event collection;
   - Verifying the existence and configuration of an audit log collection and correlation system (SIEM);
   - Assessing the SIEM's ability to analyze security events in real time;
   - Reviewing the effectiveness of incident alerting and response mechanisms;
   - Identifying potential deficiencies in the process of reporting and investigating suspicious events.
k. Malware protection solutions:
   - Verifying the existence of antivirus and anti-malware solutions implemented on workstations, servers and other critical devices;
   - Evaluation of virus signature update policies and proactive threat detection mechanisms.
l. IT infrastructure resilience assessment (Stress-Test).

2.3. **Evaluation of Staff Awareness and Cybersecurity Training Programs**

The assessment of staff awareness and training programs in the field of cybersecurity shall include the following elements:

- Analysis of training needs specific to each role within IP CBI (approximately 200 roles for around 900 employees), including those in leadership positions;

- Evaluation of the baseline knowledge level in cybersecurity for each employee category to tailor training programs effectively;

- Development of detailed long-term training and awareness plans, including courses, educational activities, and mechanisms for testing their effectiveness;

- Implementation of practical training programs designed to foster a proactive mindset towards cyber threats and to enhance incident response capabilities;
Establishment of clear control and measurement mechanisms for the effectiveness of awareness and training programs to ensure the continuous improvement of awareness levels.

3. REQUIREMENTS FOR THE CONSULTANT

3.1. **Provider Experience:**

a. Minimum 5 years of experience in IT audit;
b. At least 3 completed audit projects in the last 5 years, with at least one involving complex integrated IT systems (including databases, web interfaces, automated processes);
c. Experience in successfully completing audits of information system(s) in the public sector or for governmental institutions will be considered an advantage;
d. Experience with integrated information systems linked to government platforms in the Republic of Moldova, such as MCloud, MConnect, MPay, MPass;
e. Participation in similar projects in other countries of the region (EU, Eastern Europe) in the field of cadastre or digital public administration will be considered an advantage.

3.2. **Team Requirements:**

a. All team members must be able to communicate and draft documents in Romanian;
b. Knowledge of Russian and English will be considered an advantage;

No	Position	Responsibilities	Requirements
1	Project Coordinator / Senior Consultant	Leads the team, manages relationship with IP CBI, supervises overall audit, drafts strategic conclusions and recommendations.	Experience in IT project management, PMP/PRINCE2 certifications, excellent analytical and communication skills.

No	Position	Responsibilities	Requirements
2	IT Audit Expert / CISA	Conducts system evaluation regarding security, internal control, and IT risks.	CISA certification, experience in IT audit, solid knowledge of IT governance.
3	Technical Expert – IT Architect	Evaluates the technological architecture of systems, identifies integration points and potential infrastructure vulnerabilities.	Advanced knowledge of IT architectures, databases, cloud systems, APIs, MCloud/MConnect.
4	GIS/Cadastre Systems Expert	Analyzes graphic systems, plan layers, registration and real estate valuation systems.	Experience with GIS platforms, PostgreSQL/PostGIS, cadastral systems, spatial data modeling, Oracle DB, APEX, JavaScript, PHP, Microsoft SQL Server, C#
5	Cybersecurity Expert	Assesses security risks, access control, protection of personal data, and system integrity.	Certifications like ISO/IEC 27001, CEH or CISSP, experience in vulnerability testing and analysis. Experience with the technical platforms, inlcuding APEX, Oracle DB
6	Business / Functional Analyst	Analyzes system usage, user requirements, data flows between departments.	Experience in business process analysis and institutional digitalization. Knowledge of documentation and business process modeling tools (e.g., UML, BPMN, Microsoft Visio, Visual Basic, PostgreSQL). Experience with Java, JavaScript, Microsoft SQL Server, ELO Digital Office Enterprise 2011

The contract will be concluded for a period of **13 weeks**.

The assignment start date is expected to be no later than **July 31st, 2025**.

The detailed Terms of Reference (TOR) for the assignment can be found at the following website: https://www.ipcbi.gov.md/ro/pief/procurari/anunturi, or can be requested at the address:

e-mail: pief.procurement@ipcbi.gov.md
egor.russu@ipcbi.gov.md

Public Institution "Real Estate Cadastre" 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.

The attention of interested Consultants is drawn to paragraph 3.14, 3.16 and 3.17 of the World Bank's Procurement Regulations for IPF Borrowers - dated July 2016, revised November 2017 ("the Regulations"), setting forth the World Bank's policy on conflict of interest.

Expressions of interest must be delivered in a written form **by e-mail** by ***07.07.2025, 11:00 Local Time***

Public Institution Real Estate Cadastre

Land Registration and Property Valuation Project

Egor RUSSU, Procurement specialist

e-mail: pief.procurement@ipcbi.gov.md

egor.russu@ipcbi.gov.md

During office time hours 09:00 to 17:00 Chisinau time at the address: MD-2004, Republic of Moldova, Chisinau city, Serghei Lazo 48 str., 4th floor

Terms of Reference

Data limit?
07.07.2025 11:00