Republic of Serbia

Republic Geodetic Authority (RGA)

Second Real Estate Management Project

Terms of Reference

for

Consultant Services – Company

Quality Assurance and Quality Control
of IT Systems and IT Infrastructure Monitoring System

June 2026

Contents

I Background

The Republic of Serbia and the International Bank for Reconstruction and Development (Hereinafter: IBRD) concluded the Loan Agreement (Hereinafter: LA) for the Second Real Estate Management Project in Serbia (Hereinafter: The Project), signed by the two parties on August 21st, 2024 and ratified by the Parliament of the Republic of Serbia in its session on November 27th, 2024 ("Official Gazette RS – International Agreements", No 9/2024 of December 3rd, 2024).

The implementation of The Project has been entrusted to the Republic Geodetic Authority (Hereinafter: RGA). A Project Council and a Project Steering Committee are supervising the Project implementation.

The Project consists of three components: (A) Implementation of the Property Mass Valuation System; (B) Integration of Information Systems and the NSDI Services Development; and (C) Institutional Improvement, RGA Sustainability and Project Management.

The Project Development Objectives are to improve the transparency, accessibility, and reliability of Serbia's real property management systems.

A full description of the Project is provided in the document "Project Appraisal Document" (PAD) [1] and Loan Agreement (LA) [2]. The PAD is considered as a part of the necessary background materials to be understood by Consultants.

Implementation is entrusted to the Republic Geodetic Authority (Hereinafter: RGA).

II General Objectives

The main objective of this Quality Assurance/Quality Control (QA/QC) activity is to ensure that the software developed under the Second Real Estate Management Project (National Information System of Real Estate Cadastre of the Republic of Serbia (hereinafter: ISREC), continuation of ISREC Phase 3, and the Information System for Infrastructure Cadastre (hereinafter: ISIC)) meets the functional requirements outlined in the Technical Specification. Additionally, the Consultant will ensure quality control and support for the implementation of the IT Infrastructure Monitoring (hereinafter: ITIM) system. While ISREC and ISIC are core components of the RGA's cadastral system, the ITIM system serves as a proprietary solution supporting stable and reliable network and IT infrastructure operation.

A key new component of the Project is the development of ISIC, an internal production system intended to manage all infrastructure data within the territory of the Republic of Serbia. The Infrastructure Cadastre is integrated with the existing ISREC and serves as a unified official registry for documenting above-ground and underground infrastructure, registering ownership, real rights, and encumbrances. It ensures comprehensive spatial management, improves construction safety, and facilitates secure transactions in line with the upgraded framework for standardized registration and governance of complex infrastructure objects. ISIC data will be shared with external users through distribution services such as GeoSrbija.

The QA/QC oversight also includes the assessment of the completed national-level implementation of National ISREC, including additional requirements defined in the contract.

The consultant firm (hereinafter: the Consultant) shall support the RGA Sector for Digital Transformation and the PIU IT expert throughout the development and implementation of IT systems, including support in contract management, and in the review and assessment of system architecture, source code,

[1] https://www.rgz.gov.rs/content/images/stranice/dokumenta/2025/P500611%20-%20PAD%20-%20Official%20(Eng)%20WEB%20version.pdf

[2] https://www.rgz.gov.rs/content/images/stranice/dokumenta/2025/P500611-%20REMP2%20-%20Official%20(Eng).pdf

implementation, integration, and performance of ISREC and ISIC, while ensuring usability, effective use, quality, and compliance of these systems and ITIM, and maintaining compliance with technical workflows and defined business processes and roles.

The Consultant shall develop and implement a QA/QC plan for ISIC and National ISREC, acceptable to RGA, building upon the foundations and lessons learned from the previously executed plans for ISREC Phases 2 and 3.

Beyond technical auditing, the Consultant shall provide specialized assistance to the RGA regarding oversight of the ICT infrastructure and the existing and newly developed IT systems and digital services. A key element of this is supporting the RGA in establishing its own internal IT governance over ITIM. This includes defining clear operational protocols, performance benchmarks, and decision-making hierarchies to ensure that the RGA can independently monitor, manage, and sustain its ICT ecosystem.

III Specific Objectives

ISO/IEC 25010 (or another relevant standard such as ISO/IEC 9126 or FURPS) shall define the specific objectives of the assignment. In addition, the Consultant shall:

1. Review the system architecture and report recommendations to the Sector for Digital Transformation;
2. Synchronize development and implementation between National ISREC and ISIC;
3. Maintain compatibility between National ISREC and ISIC with IT systems implemented under the first Real Estate Management Project:
    - **Phase 1** – implementation of the workflow, DMS, UMS, and Coding System. ***This phase was completed*** under a separate contract prior to the start of Phases 2 and 3;
    - **Phase 2** – creation of the address registry and registry of administrative units;
    - **Phase 3** – core cadastre functionalities (REC alphanumerical and graphical data modules, persons, data migration, and integration with other systems).
4. Provide written recommendations for the operational acceptance of each system component, as well as for the entire system;
5. Provide support in the finalization of contracts for the implementation of ISIC and National ISREC.
6. Facilitate and assess ITIM implementation and operation in accordance with approved technical specifications, contractual requirements, practical needs of information systems that are in production and applicable standards;
7. Assist RGA in final reporting to the World Bank.

The audit will cover the delivered production versions of the ISIC and National ISREC source code delivered prior to the start date of the Audit Report activity specified below. These versions will remain unchanged during the audit, except where emergency fixes are required. Subject to the availability and support of the software developers, the audit approach may include a preliminary analysis identifying source code improvements that do not introduce risks to system operation or stability. The final audit report shall describe the implemented enhancements and assess the adequacy of the improved software for acceptance.

During the ITIM audit, the infrastructure and systems shall remain largely unchanged, except where modifications are required to ensure operational continuity, security, or the resolution of major incidents. The ITIM audit shall also confirm whether the observed network and IT components, their ITIM configurations, monitoring tools, and related documentation ensure stable, assured (in terms of necessary and available IT resources), and reliable operation of ISIC and National ISREC.

IV Tools for Audit and Parameters

The Consultant shall specify the most appropriate tools and parameters for software quality analysis in the initial Quality Audit Work Plan. The items described below shall serve as guidance.

1. Perform Analysis of National ISREC and the Infrastructure Information System

The Consultant must assess and reach conclusions about the quality of the IT systems by reviewing the software tools, software layer architecture, and overall quality, as well as performing source code artifact analysis.

Analysis of the source code can be carried out with a variety of semi-automatic tools or manually, provided that metrics are generated for the chosen Quality Profile (see below). The Consultant must advise on and reflect on the type of metrics and their thresholds to be used in the Quality Profile, and assess the actual values for the software source code under analysis. For example, a Quality Profile contains desired thresholds for:

a) ERROR! REFERENCE SOURCE NOT FOUND.

This metric refers to the comment-to-code ratio. Good programming practice requires at least 70% relevant comments in the code. The Consultant must assess the comments used in the software source code.

b) COMPLEXITY

The number of branching statements determines source code complexity (if, for, while…). General indicators for source code complexity are 1-4 branching statements for low complexity, 5-7 for moderate complexity, 8-10 for high complexity, and 11+ assessed as very high complexity. The Consultant must assess the complexity of the software source code.

c) NUMBER OF CLASSES

This metric shows the total number of classes, packages, and methods, as well as the total number of getters and setters. Good programming practice suggests that a class should fit within a single screen; the average lines of code (LOC) per class should not exceed 100. The Consultant must assess the number of classes, packages, and methods, including getters and setters, used in the source code.

ERROR! REFERENCE SOURCE NOT FOUND.The Response for Class (RFC) metric gives the total number of responses of a class to other classes. If the RFC for a class is large, it indicates high complexity, which may cause maintainability issues. Good practice suggests that this value for a class should not exceed 100. The Consultant must assess class responses used in the software source code.

d) SOURCE CODE RULES

This metric refers to the level of compliance withsource code rules, such as those used in rule engines like Checkstyle, PMD, and FindBugs. The Consultant must define a basic set of rules to be part of the Quality Profile for the assessed software.

e) LACK OF COHESION OF METHODS

This metric refers to the cohesiveness property of classes and indicates the number of connected components in a class. A connected component is a set of related methods and fields. There should be only one such component for each class. If there are two or more components, the class should be split into smaller classes. Low cohesion means that the component’s contents are an unrelated jumble of actions, often grouped together due to time dependencies or convenience. The Consultant must assess the degree of cohesion in the software source code.

f) PACKAGE TANGLE INDEX

This index refers to how tangled the software packages are; ideally, there should be no cycles. This metric provides the values of dependencies to be removed in order to achieve a less tangled package structure. The Consultant must assess this index in the software source code.

g) TEST CASE AND UNIT TEST COVERAGE

This metric shows coverage of each function, statement, decision, and condition in unit testing, also known as white-box testing. Good practice dictates that test cases and unit tests should cover at least 80% of the entire source code. The Consultant must select relevant examples of test case and unit test coverage in the software.

A crucial element of the source code audit is the severity analysis of detected issues, with primary focus on Blocker and Critical findings to prevent production failures, security breaches, and maintenance problems. These high-priority defects must be treated as severe events requiring immediate resolution before final acceptance. A proactive assessment of Major issues shall ensure they do not affect core operation or software usage. Confirming that code defects do not degrade performance or user experience enables the software team to maintain delivery velocity without compromising operation or maintainability. This tiered approach ensures that high-risk findings are eliminated while remaining issues do not interfere with reliable system operation.

2. Methodology for Software Product Quality Audit

The Consultant shall review software quality based on a clear and transparent standard or methodology. ISO/IEC 25010 may be considered, as well as ISO/IEC 9126 or FURPS. **ISO/IEC 25010 defines s**ystem and software quality models comprising characteristics and sub-characteristics for software product quality and software quality in use. It is an international standard for the evaluation of software quality3, 4, distinguishing between product quality (Functional Suitability, Performance Efficiency, Compatibility, Usability, Reliability, Security, Maintainability, and Portability) and quality in use (Effectiveness, Efficiency, Satisfaction, Freedom from Risk, and Context Coverage).

Software architecture and product quality attributes that must be assessed are related to:

a) FUNCTIONAL SUITABILITY

Each characteristic and its sub-characteristics shall be assessed in accordance with ISO/IEC 25010 definitions.

b) SECURITY

Information systems in production are established as "a sophisticated security organization with respect to hardware, network, software application, database, and data." The Consultant must therefore pay particular attention to:

- Confidentiality,
- Integrity,
- Non-repudiation,
- Accountability,
- Authenticity.

c) RELIABILITY

Reliability defines the capability of the software to maintain its service provision under defined conditions for defined periods through the following attributes:

- Maturity,
- Availability,
- Fault tolerance,
- Recoverability.

---

[3] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35733

[4] http://iso25000.com/index.php/en/iso-25000-standards/iso-25010?limit=3&limitstart=0

d) ERROR! REFERENCE SOURCE NOT FOUND.

Usability exists only in relation to functionality and refers to the ease of use for a given function. The ability to learn how to use software (learnability) is also a major sub-characteristic of usability:

- Appropriateness recognizability,
- Learnability,
- Operability,
- User error protection,
- User interface aesthetics,
- Accessibility.

e) PERFORMANCE EFFICIENCY

This characteristic concerns the system resources used when providing the required functionality. The amount of disk space, memory, network capacity, etc. provides a good indication of this characteristic. The attributes bearing on the relationship between the level of performance of the software and the amount of resources used under stated conditions are:

- Time behavior,
- Resource utilization,
- Capacity.

f) MAINTAINABILITY

Serviceability, often termed supportability, is the ease with which repair and maintenance can be performed. The ability to identify and fix a fault within a software component is addressed by maintainability. Maintainability is impacted by code readability, complexity, and modularization. See the previous section "Perform Analysis of ISREC" in relation to:

- Modularity,
- Reusability.
- Analyzability,
- Modifiability,
- Testability.

g) COMPATIBILITY

The degree to which a product, system, or component can exchange information with other products, systems, or components, and perform its required functions while sharing the same hardware or software environment. This characteristic comprises the following sub-characteristics:

- Co-existence,
- Interoperability.

h) PORTABILITY

Portability defines the level of effectiveness and efficiency with which a system, product, or component can be transferred from one hardware, software, or other operational or usage environment to another. This characteristic is composed of the following sub-characteristics:

- Adaptability,
- Installability,
- Replaceability.

3. Provide Conclusion on Deliverable Quality

The Consultant shall provide recommendations on how system acceptance and improvement should proceed following the evaluation.

This risk register will detail each risk, its likelihood, severity, and impact, together with mitigation measures and assigned responsibilities for risk reduction or elimination.

V Scope of Work and Tasks

If not present on RGA premises, the Consultant shall be available for communication via email, chat, or telephone during working hours throughout the contract duration.

The Consultant will support RGA and PIU in contract management, project management, monitoring, supervision, and quality control/quality assurance for the implementation of the IT systems.

The Consultant shall assess the adequacy and effectiveness of RGA governance, risk management, and control processes in providing reasonable assurance regarding the effectiveness of implementation in accordance with the technical specifications and implementation schedule for the IT systems.

The Consultant shall perform the following tasks:

1. Support RGA in contract management;
2. Provide support and assistance to the PIU IT Expert;
3. Review database design and its compliance with the overall ISREC data models as well as its compliance with the ISO 19152, Land Administration Domain Model (LADM).;
4. Prepare, revise, and verify quality standards and test procedures for software design and source code evaluation
5. Review newly developed or updated software code, including documentation, diagrams, and flowcharts, to determine whether the code performs in accordance with user requirements and complies with established guidelines;
6. Recommend software code improvements or corrections to the supplier and RGA;
7. Review software operation and monitoring logs to identify processing errors;
8. Consult with RGA testers and users regarding validity of results, accuracy, adequacy, reliability, and conformance to established standards;
9. Identify differences between standards and user applications, and propose modifications to ensure compliance with standards;
10. Identify and report potential risks;
11. Conduct compatibility assessment of components developed across all ISREC phases and ISIC;
12. Monitor ISREC performance after rollout to prevent recurrence of operational issues and ensure efficienct operation;
13. Review training documentation and user manuals for all RGA consultants prior to rollout
14. Support RGA staff in preparing final acceptance of National ISREC and ISIC following final testing at RGA headquarters for a period of four weeks after completion of rollout and training in local offices, as per the contract site table.
15. Perform quality control of ITIM system;
16. Support the operation and maintenance of the ITIM system in accordance with the requirements set out in Annex 1.

VI Implementation Schedule

a) National Information System of Real Estate Cadastre (National ISREC)

Line Item No.	**Subsystem / Item**	Site / Site Code	Delivery (Bidder to specify in the Preliminary Project Plan)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
I.	**Inception phase including Project plan**	RGA HQ	W2	-	W4	
II.	**New and improved functionalities**	RGA HQ	W4	-	W30	
1.	**Additional Development of application for optimization of the working processes**	RGA HQ	W4	-	W10	
2.	**Operational acceptance #1**	RGA HQ	W11	-	W12	yes
3.	**Development of new functionalities of application**	RGA HQ	W11	-	W24	
4.	**Operational acceptance #2**	RGA HQ	W25	-	W26	yes
5.	**Development of new transformation procedures to optimize transformation process**	RGA HQ	W25	-	W32	
III.	**Operational acceptance #3**	RGA HQ	W33	-	W34	yes
IV.	**Transformation in the LCO**	RGA HQ LCOs	W2	W2	W154	
1.	Group of LCOs 1	RGA HQ LCOs	W2	W14	W15	
2.	**Operational acceptance for LCOs 1**	RGA HQ	W3	W14	W15	
3.	Group of LCOs 2	LCOs	W15	W37	W38	
4.	**Operational acceptance for LCOs 2**	RGA HQ	W16	W37	W38	
5.	Group of LCOs 3	LCOs	W38	W70	W71	
6.	**Operational acceptance for LCOs 3**	RGA HQ	W39	W37	W38	
7.	Group of LCOs 4	LCOs	W71	W92	W93	
8.	**Operational acceptance for LCOs 4**	RGA HQ	W72	W92	W93	
9.	Group of LCOs 5	LCOs	W93	W128	W129	
10.	**Operational acceptance for LCOs 5**	RGA HQ	W94	W128	W129	
11.	Group of LCOs 6	LCOs	W129	W151	W152	
	Operational acceptance for LCOs 6	RGA HQ	W130	W151	W152	
V.	**FINAL OPERATIONAL ACCEPTANCE OF THE SYSTEM**	RGA HQ LCOs	W153	W154	W154	

Table 1 – Implementation schedule for the National Information System of Real Estate Cadastre

b) Information system for infrastructure Cadastre (ISIC)

Line Item No.	Subsystem / Item	Site / Site Code	Delivery (Bidder to specify in the Preliminary Project Plan)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
1.	Project preparation phase	RGA		W1-2	W3	
2.	Detailed Business analysis for the ISIC	RGA		W2-6	W7	
3.	Design, development, integration and installation	RGA		W08-38	W39	
4.	Final verification of solution and user training	RGA		W40-42	W42	
5.	System implementation, with post-support (stabilization phase)	RGA		W42-48	W46-48	
6.	**OPERATIONAL ACCEPTANCE OF THE WHOLE SYSTEM – Final Operational Acceptance**	RGA		W48	W48	
6.	Warranty period	RGA		W48- W100		

Table 2 – Implementation schedule for the Information system for infrastructure Cadastre (ISIC)

c) Quality Assurance and Quality Control (QA/QC) of IT Systems and ITIM

No	Task	Start date	Duration	Working days	Finish	Acceptance
I.	Overall Work Plan	W1	5 WEEKS	10	W5	W6
II.	Audit Report (National ISREC) – Development of New Transformation Procedures To Optimize The Transformation Process (change of migration procedures and review of daily controls)	W3	5 WEEKS	20	W7	W8
III.	Audit Report – Quality Control of ITIM System	W3	5 WEEKS	15	W7	W8
IV.	Audit Report (ISIC) – Work Plan	W3	9 WEEKS	10	W11	W12
V.	Report – Improvement of the ITIM System	W3	10 WEEKS	30	W12	W13
VI.	Milestone – Maintenance of the ITIM System	W3	127 WEEKS		W129	W130

6.1	W3-W27	W3	25 WEEKS	12	W27	W28
6.2	W28-W52	W28	24 WEEKS	12	W52	W53
6.3	W53-W77	W53	25 WEEKS	12	W77	W78
6.4	W78-W103	W78	26 WEEKS	12	W103	W104
6.5	W104-W129	W104	26 WEEKS	12	W129	W130
7.	Audit Report (National ISREC) – Preliminary Implementation of the System Based on Experiences from Implemented LCOs	W3	23 WEEKS	12	W25	W26
8.	Audit Report (ISIC) – Design, Development, Integration, and Migration of Data	W11	27 WEEKS	18	W37	W38
9.	Audit Report (ISIC) Verification of the Solution, User Training, System Commissioning, and Final Acceptance	W47	3 WEEKS	8	W49	W50
10.	Audit Report (National ISREC)I –Final Report for Implementation in all LCOs	W27	23 WEEKS	20	W49	W50
11.	Audit Report – Quality Control of ITIM System	W52	40 WEEKS	20	W91	W92
12.	Audit Report – Final Quality Control of ITIM System	W93	37 WEEKS	20	W129	W130
13.	Final Report of the Overall QA/QC **C**onsulting Service	W128	2 WEEKS	5	W129	W130

Table 3 – Implementation schedule for QA/QC

1. The Consultant will deliver a Work Plan within the first five (5) weeks of the Contract start date (W1–W5). RGA will provide comments and/or accept the Work Plan within five (5) days of delivery (by W6).
2. The Audit Report (National ISREC) – Development of New Transformation Procedures To Optimize The Transformation Process (including change of migration procedures and review of daily controls) will be delivered by the end of the 7th week (W7) of the Contract start date.
   RGA will provide comments and/or accept the Audit Report within five (5) days of delivery (W8).
3. The Audit Report – Quality Control of ITIM System will be delivered by the end of the 7th week (W7) of the Contract start date.
   RGA will provide comments and/or accept the Audit Report within five (5) days of delivery (W8).
4. The Audit Report (ISIC) – Work Plan will be delivered by the end of the 11th week (W11) of the Contract start date.
   RGA will provide comments and/or accept the Audit Report within five (5) days of delivery (W12).

5. The Report – Improvement of the ITIM System will be delivered by the end of the 12th week (W12) of the Contract start date.
   RGA will provide comments and/or accept the Report within five (5) days of delivery (W13).
6. Maintenance of the ITIM System will be carried out continuously from W3 to W129, with final acceptance at W130. Milestones will be notified for every 25 or 26-week period, with RGA acceptance during the following week.
   This activity includes preventive and corrective maintenance, system updates, and incident management, ensuring reliable and uninterrupted system operation.
7. The Audit Report (National ISREC) – Preliminary Implementation of the System Based On Experiences from Implemented LCOs will be delivered by the end of the 25th week (W25) of the Contract start date.
   RGA will provide comments and/or accept the Audit Report within five (5) days of delivery (W26).
8. The Audit Report (ISIC) – Design, Development, Integration, and Migration of Data will be delivered by the end of the 37th week (W37) of the Contract start date.
   RGA will provide comments and/or accept the Audit Report within five (5) days of delivery (W38).
9. The Audit Report (ISIC) – Verification of the Solution, User Training, System Commissioning, and Final Acceptance will be delivered by the end of the 49th week (W49) of the Contract start date.
   RGA will provide comments and/or accept the Audit Report within five (5) days of delivery (W50).
10. The Audit Report (National ISREC) – Final Report for Implementation in all LCOs will be delivered by the end of the 49th week (W49) of the Contract start date.
    RGA will provide comments and/or accept the Audit Report within five (5) days of delivery (W50).
11. The Audit Report – Quality Control of ITIM System will be delivered by the end of the 91st week (W91) of the Contract start date.
    RGA will provide comments and/or accept the Audit Report within five (5) days of delivery (W92).
12. The Audit Report – Final Quality Control of ITIM System will be delivered by the end of the 129th week (W129) of the Contract start date.
    RGA will provide comments and/or accept the Audit Report within five (5) days of delivery (W130).
13. The Final Report of the Overall QA/QC Consulting Service will be delivered at W129, with acceptance at W130.

This report shall summarize all activities undertaken within the contract and demonstrate how project objectives and outputs were achieved.

All reports and documentation, in English and Serbian, are to be submitted in electronic format together with signed paper copies in both languages to RGA management. Monthly reports shall be submitted only in Serbian and in electronic format. The prepared reports shall be concise and focused on the particular phases of implementation.

Based on this documentation, RGA officials will sign or reject the acceptance certificate for the delivered IT system.

VII Deliverables

The Consultant will be responsible for delivering the following reports for each phase:

- **Work Plan** – within the first weeks of the Contract start date. The Work Plan is subject to approval by RGA officials;
- **Inception Report**;
- **Ad hoc reports** – when urgent issues must be addressed if a problem arises or when a risk to implementation becomes visible;
- **Monthly reports related to ISIC and National ISREC**:
    i. Summary of Project progress indicating key challenges and recommendations for implementation;
    ii. Reports on how the team is complying with the Project plan;
    iii. Recommendations and methodology for training;
    iv. Reports to RGA staff on the progress of testing;
    v. Updates of the Risk Management Plan as needed;
    vi. Suggestions for general quality policies, procedures, and practices to be followed by partners throughout the duration of the Project;
    vii. Change requests focused on the changes that need to be made in the Project plan or execution to produce better products and prevent defects;
- Audit Report will include[5]:
    i. A report to RGA on the technical quality audit of the source code, software architecture, and technical documentation of ISREC and ISIC;
    ii. A report regarding database design (DB for Infrastructure) and its compliance with the ISREC data model implemented under Phases 1, 2, and 3;
    iii. A certificate of testing, which is a written document containing the Consultant's confirmation that the delivered IT system is in accordance with the prescribed technical specification and fulfills all necessary functions for smooth operation of the ISREC system;
    iv. A written document outlining the procedure for the final acceptance of the National ISREC and the Infrastructure Information System;
    v. A report on the technical quality of ITIM system.
- **Final Report**.

The Audit Report shall state the scope, objectives, period of coverage, and the nature, timing, and extent of the audit work performed.

The Report shall state the findings, conclusions, and recommendations, and any reservations, qualifications or limitations in scope that the Consultant has with respect to the audit.

The Consultant shall discuss the draft report contents with management in the subject area prior to finalization and release and include management's comments in the final report wherever applicable.

Reports shall be addressed to the appropriate management for necessary action. A listing of all issues raised during the review may be issued.

[5] Consultant will produce contract requirements tracking table with all contract requirements and indication of the status: met/not met, accepted/rejected/conditionally accepted or cancelled with a ref. to the contract amendments for any changes of the contract requirements. Recommendations on how to proceed with the requirements, which are not met are important part of the report.

VIII Period of Performance

The assignment duration is 130 weeks and covers the contract duration of both the National ISREC and ISIC. The duration may be extended depending on the implementation of the ISREC and ISIC software and the needs of ITIM system.

The assignment is expected to start immediately after Contract signing.

A Consultant will be selected in accordance with the CQS procedure set out in the World Bank's "Procurement Regulations for IPF Borrowers" (February 2025).

IX Qualifications of the Consultant

The Consultant must have at least 10 years of experience in consulting services, demonstrated by company references, in conducting technical quality audits of multi-agency information systems, including consulting in developing IT service management.

The Consultant must have:

- ISO/IEC 9000, ISO/IEC 20000 and ISO/IEC 27000 or equivalent certification
- IT system analysis using automated tools
- Software architecture analysis
- Application and infrastructure performance testing
- ITIM development and implementation

The Consultant must demonstrate proven experience in software quality control, IT service management and system improvement within the last 10 years on systems of comparable complexity and size.

The Consultant must have a strong and relevant track record in ICT projects with public sector institutions, including contract management, software solution implementation, staff training, handover, and product acceptance.

In addition to ICT project management skills, the Consultant must have experience with international cooperation projects or clients, with emphasis on quality standards, monitoring, and reporting.

The Consultant must provide a team that meets the following requirements:

Senior Software Quality Audit Expert

Minimum Requirements:

- At least 10 years of IT experience, with a proven record in software development and/or implementation
- At least 3 years of experience in quality control of web-based software and IT architecture projects
- At least 3 years of experience in technical quality audits of complex information systems
- Qualifications in IT governance frameworks such as ITIL or COBIT, specifically related to system oversight and maintenance, with the ability to define service KPIs and translate them into monitoring metrics
- Proven ability to develop Standard Operating Procedures (SOPs) and governance protocols enabling effective management of IT assets or services and strengthening internal ownership and knowledge
- Strong knowledge of systems engineering concepts

Considered an Advantage:

- Strong written and verbal communication skills, with a documented track record in technical reporting and specification or dissemination of complex technical or governance concepts aligned with best standards applied in international cooperation projects
- Comprehensive knowledge of web application and service-related hardware and software configuration
- Previous experience with QA/QC and cadaster and property registration systems

Senior IT Infrastructure Specialist

Minimum Requirements:

- At least 5 years of experience in auditing and testing enterprise-grade networks, including expertise in implementing, auditing, and optimization of IT Infrastructure Monitoring System (ITIM) platforms for high-availability web services, including hands-on experience adding monitoring nodes or reconfiguring equipment to ensure system visibility
- Comprehensive knowledge of IT architecture components related to performance, security, authorization, and authentication, supported by operational experience in system oversight and maintenance of complex IT environments
- At least 3 years of experience in network configuration, IT resource management, and load balancing, including management of distributed monitoring for remote workstations using both thick and thin clients
- Demonstrated experience testing the functionality, performance, and resilience of networked systems, including defining operational limits, setting alert thresholds, and contributing to technical incident response based on monitoring
- Proven ability to collaborate with institutional staff to strengthen their technical capacity through knowledge transfer, implementation of ITIM best practices, and ensuring a response to infrastructure events
- Proven ability to develop, support, and implement SOPs and governance protocols, including clear guidance on integration of monitoring processes and day-to-day management of IT infrastructure and services

Anex 1

Maintenance and Support for IT Infrastructure Monitoring System

I. General Technical Requirements

IT Infrastructure Monitoring System (ITIM) of the Republic Geodetic Authority (RGA) implies centralized monitoring of the entire IT infrastructure, including monitoring of the computer network, physical infrastructure in the data center and servers, as well as analysis of network traffic structure and network events. Such a monitoring system effectively supports the detection and resolution of issues related to IT infrastructure and performance problems.

Maintenance and support services for the IT infrastructure monitoring (ITIM) system of the Republic Geodetic Authority include the following applications, with licenses without limitations:

- Network Monitoring System
- NetVizura NetFlow Analyzer
- NetVizura EventLog Analyzer

2. Network Monitoring System

Monitoring enables continuous collection of performance values from devices, visualization of values (including graphical charts within a selected time interval), definition of alarms based on various complex criteria, etc.

- Delivery of licenses for the latest version of the application, without time or usage limitations (perpetual, unlimited).
- Installation of the latest version of the application, including updates of system libraries and security patches.
- Implementation of the application with updating of monitoring system data.

3. NetFlow Analyzer System

Analyzes network traffic based on standard data exported by NetFlow, IPFIX and sFlow protocols. It collects and processes raw NetFlow data; stores and enables efficient review of individual files; displays active and all registered alarms and sends email notifications to selected users; generates and exports statistics in PDF format, etc.

- Delivery of licenses for the latest version of the application, without time or usage limitations (perpetual, unlimited).
- Installation of the latest version of the application, including updates of system libraries and security patches.
- Implementation of the application with updating of monitoring system data.

4. EventLog Analyzer System

Supports the collection, archiving and analysis of events within the network and IT environment, through standard Syslog and SNMP TRAP messages, according to the specified requirements, etc.

- Delivery of licenses for the latest version of the application, without time or usage limitations (perpetual, unlimited).

- Installation of the latest version of the application, including updates of system libraries and security patches.
- Implementation of the application with updating of monitoring system data.

5. Maintenance of the Software System

- Expert assistance in using infrastructure analysis applications in case of incident situations, during business hours, up to 10 tickets per month;
- Maintenance of system functionality, including delivery of new application versions, when available;
- Correction of software system errors identified during operation;
- Professional telephone support;
- On-site intervention as needed and in agreement with the Client;
- Troubleshooting through provision of first-, second-, and third-level support services.

6. IT Infrastructure Monitoring Software System – Service Level Agreement (SLA)

The Bidder is obliged to provide 24 hours a day, 7 days a week, 365 days a year, support during the duration of the contract with response, recovery and resolution times for any problems that arise within the following deadlines:

Severity Level	**Description**
1 – Critical (Business Interruption)	• Partial or complete non-operability of the software system with critical consequences for the Client's business operations (e.g. inability to monitor network devices, vital RGA services, or use essential databases). • Circumstances resulting in significant or critical business impact for the Client due to partial or complete failure (malfunction or operational issue) of communication devices, equipment, or software subject to monitoring. • Vital components of the network and infrastructure, key users, and services are affected. Business operations are severely degraded or fully disrupted, resulting in significant losses or complete process outage. • When reporting the issue, the Client's authorized technical representative explicitly indicates that it is a Level 1 issue. • Requires immediate intervention and bypasses standard queues.
2 – Major (Significant Risk)	• Partial non-operability where the system remains largely usable, but component failures represent a significant issue for the Client's business operations. • Circumstances resulting in limited business impact for the Client due to partial or complete failure (malfunction or operational issue) of communication devices, equipment, or software subject to monitoring. • Critical users and services are not yet affected, but there is a risk of escalation. • Requires rapid but not immediate recovery to ensure continuous business operation.
3 – Low (Minor Disturbance)	• The software remains operational, but certain components exhibit minor issues that do not affect overall functionality or intended purpose.

Severity Level	Description
	• Circumstances result in minor disturbances or reduced efficiency for a limited number of users and do not significantly affect the Client's business operations. • Vital infrastructure components under monitoring are not affected, and a limited number of users experience reduced efficiency in performing business processes. • Allows medium-term recovery to prevent prolonged impact on operational efficiency.
4 – Informational	• The software system is fully operational with no functional degradation. • Circumstances relate to clarify needs, provide advice, improve use documentation clarifications with no measurable impact on business operations, system availability, service quality, or the Client's workflows. • Vital infrastructure components and monitored services are not affected, and no disruption to business processes occurs. • These items do not require recovery. They are recorded for tracking, transparency, and governance purposes, and are prioritized based on strategic value, alignment with other planned changes, and opportunities for quick support.

The following table outlines the maximum allowable timeframes by severity level:

Severity Level	**Response Time**	**Recovery Time** (Interim Fix)	**Resolution Time** (Final Fix)
Level 1 – Critical	30 minutes	6 hours	30 days
Level 2 – Major	60 minutes	Next business day	60 days
Level 3 – Low	120 minutes	7 days	90 days
Level 4 – Informational	24 hours	N/A	On per-case basis

Communication and Escalation

To ensure a frictionless response during critical incidents, the following escalation paths are defined:

- Tier 1 (Operational): Helpdesk email, phone call, or message for initial reporting.
- Tier 2 (Technical): Lead Engineer for diagnostics exceeding two hours.
- Tier 3 (Management): Service Provider Manager for incidents affecting business-critical operations or SLA breaches, as soon as identified by the authorized Client Representative or the Lead Engineer.

This in particular reduces friction during a Severity level 1 incidents because everyone knows exactly who to call.

Detailed contact information and key personnel assignments will be formalized upon the execution of the contract.

7. Description of Requirements

- The Contractor shall provide services efficiently, with high quality and professionalism, taking into account the Client's business interests.
- The Contractor shall maintain records of reported issues and performed activities under this contract and shall periodically, or upon request, report to the Client.

- When delivering a new version of the software system, the Contractor shall provide documentation containing activation keys for the software and licenses.
- In the event of delivering a new software version, the Contractor shall provide full support to the Client during installation or perform the installation at the Client's request.
- Installation includes installation of the software systems, activation of software and licenses, configuration, and commissioning into production.
- Upon the Client's request, the Contractor shall provide users of the software system with the necessary knowledge transfer required for system usage. This obligation must be fulfilled at least once and mandatorily with each delivery of a new software version.
- The Contractor shall maintain the operating system and other system software and modules on the servers where the software system is executed, including detection of hardware issues.
- For the purpose of integration with the network monitoring system, and upon the Client's request, the Contractor shall request configuration changes to the Client's equipment.
- The Contractor shall provide expert assistance in using the software system to analyze events and conditions caused by partial or complete failure (malfunction, operational issue) of communication devices, equipment, and software subject to monitoring, in order to determine the root cause of such failures.

8. Process Explanation

- **Problem reporting** refers to the Client contacting the Contractor's Service Center via telephone, email, or web service, providing a description of the issue, its manifestation, the conditions under which it occurs, the consequences it causes, and specifying the technical severity level.
- The technical severity level is assessed by the Client when reporting the issue to the Contractor's Service Center.
- **Response time** is the time interval starting from the moment the Client's authorized expert submits the request to the Contractor's technical support center (via phone, email, web service, etc.) and ending when a qualified person capable of providing the requested service contacts the Client's authorized expert. Automated system responses from the Contractor do not count.
- **Recovery time** is the period during which the functionality of the monitoring system is restored or expert assistance is provided for analyzing the condition caused by partial or complete failure (malfunction, operational issue) of communication devices, equipment, and software subject to monitoring after the issue has been reported.
- Recovery time includes the period from acceptance of the issue report to restoration of software package functionality, as well as determination of the root cause of partial or complete failure (malfunction, operational issue) of monitored communication devices, equipment, and software.
- If system recovery requires installation of new software versions with new functionalities (software upgrade), the application of a solution that restores the system to operational status is allowed, even if it is not necessarily the final version of the software solution.
- **Resolution time** is the period from acceptance of the issue report to establishment of a condition that can be considered a final resolution of the software system malfunction, or completion of the full analysis of events and conditions caused by partial or complete failure (malfunction, operational issue) of monitored communication devices, equipment, and software during the detected failure period. If resolution requires installing a new software version with new functionality (software upgrade), installation of the latest version of the software system is assumed.
- Installation and configuration of the software package shall be performed by the Contractor on the Client's equipment.