REPUBLIC OF SERBIA

REPUBLIC GEODETIC AUTHORITY (RGA)

TERMS OF REFERENCE

FOR

IMPLEMENTATION OF INTEGRATED MANAGEMENT SYSTEM (IMS)

Belgrade, October 2022

I. Introduction and Background

The Republic of Serbia and the International Bank for Reconstruction and Development (Hereinafter: IBRD) concluded the Loan Agreement (Hereinafter: LA) for the Real Estate Management Project in Serbia (Hereinafter: The Project), signed by the two parties on April 17th, 2015 and ratified by the Parliament of the Republic of Serbia in its session on Jun 24, 2015 (Official Gazette of the Republic of Serbia – International contracts, No. 13-15).

The Law on State Surveys and Cadaster (LSSC, 2009) with appropriate amendments provides a solid foundation for the project. A viable single agency, the Serbian Republic Geodetic Authority (RGA), is implementing the LSSC. A Project Council and Project Steering Committee are supervising the Project Implementation.

The Project consists of four components: (A) Valuation and Property Taxation; (B) E-governance for Enabling Access to Real Estate Information; (C) Institutional Development of the RGA; and (D) Project Management and Support Activities.

The objective of the Project is to improve the efficiency, transparency, accessibility and reliability of the Republic of Serbia's real property management systems.

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

Implementation is entrusted to the Project Implementation Unit (Hereinafter: PIU) of the Republic Geodetic Authority.

II. Institutional Framework

RGA is a special budget-institution of the Republic of Serbia. With over 2,000 employees, it was established to perform professional state administration works pertaining to state survey, real estate cadastre, utilities cadastre, basic geodetic works, address register, topographic-mapping business, real estate valuation, geodetic-cadastral information system and National Spatial Data Infrastructure and geodetic works in engineering-technical fields.

Cadastral Services which include property rights registrations for businesses and individuals are the most important and visible services RGA provides.

The Sector for Real Estate Cadastre (REC) is the largest Sector within RGA. The REC Sector is organized territorially, with citizens' applications being processed and handled regionally. Regional real estate Cadastre offices possess 80% of the total staff members (with high education level), provide 90% of RGA services throughout the country, and generate 95% of the income of RGA. There are currently 170 local offices and RGA has a total of 2,198 staff. Annually, the offices receive 571,533 number of applications for registration of rights, 91,943 applications for issuing copies of cadastral maps, and 1,595,000 applications for property folio extracts. The headquarters of RGA, located in Belgrade, has 339 staff, and is divided into 6 sectors:

- Sector for Geodetic Works
- Sector for Professional and Inspection Supervision
- Sector for Real Estate Cadastre
- Sector for Digital Transformation
- Sector for Legal Affairs
- Sector for Development

[1] http://documents.worldbank.org/curated/en/541411468182064197/pdf/PAD955-PAD-P147050-R2015-0041-1-Box385415B-OUO-9.pdf

Smaller internal units outside of sectors are as follows:

- Department for Finance and Control
- Geospatial Data Management Center
- Department of Archives
- HR Department
- Department for Internal Auditing

III. Objective of the Consultancy:

One of the main tasks of RGA is maintenance of all the real estate data. Currently RGA uses different systems to maintain the real estate data. As RGA works to continue to meet customer and legal requirements for compliance, it is becoming more necessary for RGA as the critical infrastructure of the state to obtain and maintain multiple ISO Management System Standards implementation. RGZ as critical infrastructure is the governmental body of systems, networks and assets that are so essential that their continued operation is required to ensure the security of the state, nation, its economy, and the public's health and safety. One common combination of ISO standard implementations today that is a “must have“ for organizations of similar kind of business is ISO 9001, ISO/IEC 27001, and ISO/IEC 27701.

ISO 9001 is the internationally recognized standard for Quality Management Systems (QMS). It is the most widely used QMS standard in the world, with over 1.1 million certificates issued to organizations in 178 countries. ISO 9001 should illustrate a crystal-clear holistic approach about Quality Management System and emphasizes on the importance of ensuring to deliver nothing else than high quality products and services to RGZ’s clients. In order to ensure security of the information system of any organization, ISO 27001 should come into action by giving a systematic approach to secure RGZ’s data by filling the loopholes in current management system that may lead to data lost and hacking of may be even complete RGZ’s system and gives guidelines about managing security risks. ISO 27701 is an enhancing extension of ISO 27001. The standard should provide to RGZ the data privacy and information security standards required by Serbian Law on Personal Data Protection (ZZPL) and EU General Data Protection Regulation (GDPR). To efficiently manage privacy, it contains the structure for Personally Identifiable Information (PII) processors and controllers. Implementing ISO 27701 will create a Privacy Information Management System, or PIMS for short. Using ISO 27701 as the standard for data security should show RGZ’s customers and stakeholders that supports ZZPL and GDPR compliance and privacy legislation. Also, it ensures that RGZ should have effective systems they can trust. By reducing the potential information security and privacy risks for individuals and RGZ by using the controls, it would be created a more trustworthy brand.

The International Organization for Standardization (ISO) defines a management system as “a system in which an organization manages the reciprocal parts of its business in order to achieve its objectives.” Regarding the ISO 9001, ISO 27001, and ISO 27701 standards, though they regulate three separate management systems, they should create unique Integrated Management System (IMS).

ISO 9001 will be able to provides a framework and set of principles that ensure a common-sense approach to the management of RGZ to consistently satisfy customers and other stakeholders. In simple terms, ISO 9001 implementation provides the basis for effective processes and effective people to deliver an effective product or service time after time. The key to any successful business is strong quality control. If RGZ wants its operation to thrive, their client base must be confident that the goods or services they offer meet or exceed expected standards. ISO 9001 is a quick and easy way for current and potential clients to see if RGZ has put the time and effort into making sure that product or service is the best it can possibly be.

ISO 27001 is the international standard that provides a framework for Information Security Management Systems (ISMS) to provide continued confidentiality, integrity, and availability of information as well as legal compliance. ISO 27001 certification will be an essential for protecting RGZ's most vital assets like employee and client information, brand image and other private information. The ISO standard includes a process-based approach to initiating, implementing, operating, and maintaining the ISMS. ISO 27001 implementation in RGZ is an ideal response to customer and legal requirements such as the ZZPL and GDPR and to potential security threats including cybercrime, personal data breaches, vandalism, terrorism, fire, damage, misuse, theft, and viral attacks.

ISO 27701 is a data privacy extension to ISO 27001. This newly published information security standard will be able to provide guidance for RGZ looking to put in place system to support compliance with ZZPL and GDPR personal data privacy requirements. ISO 27701, also abbreviated as PIMS (Privacy Information Management System) outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage data privacy. Privacy information management systems are sometimes referred to as personal information management systems. This will reduce risk to the privacy rights of individuals and to RGZ by enhancing an existing Information Security Management System. This standard is a great way of demonstrating to customers, external stakeholders, and internal stakeholders that effective systems are in place to support compliance to ZZPL and GDPR privacy legislation.

IV. Scope of Work

The Consultant will closely cooperate with RGA and relevant stakeholders in implementing ISO 9001, ISO/IEC 27001 and ISO/IEC 27701 international standards and create unique Integrated Management System (IMS). Selected Consultant shall provide input and support to RGA in the following way:

- Get Top Management on Board and making sure that the people at the top of RGZ management understand what IMS means for its business because without everyone completely committed it becomes much more difficult to affect change throughout the business
- Preparation of GAP analyses of the current situation. Once have everyone on board analyze the current system and compare it to the ISO 9001, ISO 27001, and ISO 27701 standards
- Plan everything out for Implementation and having a solid plan in place is essential to making the transition to a new QMS against ISO 9001, to a new ISMS against ISO 27001 and to a new PIMS against ISO 27701 i.e., to a new integrated management system (IMS)
- Decide on an implementation team to begin implementation by top management who should decide on and create the implementation teams for ISO 9001, ISO 27001, and ISO 27701. These teams should be made up of managers from different areas of RGZ business
- Identify core and support processes and map out a plan for meeting ISO 9001, ISO 27001, and ISO 27701 standards and be aware of which processes within RGZ coordinate with which requirements
- Get everyone involved where every single person that works within RGZ should be aware that change is coming with ISO 9001, ISO 27001, and ISO 27701
- Provide employee training, which is crucial to keeping IMS running, and train all of employees on the parts of the system that are specific to their area of work. Training should teach the employees about the procedures that apply to their work, which forms they should be using and how to complete and process them, how to find any specific IMS documented

information and how it relates to their position, how to report issues so that they can be fixed, where to find all relevant documents for conducting the internal audits

- Identify objectives and responsibilities, develop documented information such as policies, procedures, and instructions with following records within RGZ as an integral part of keeping the business committed to meeting requirements of ISO 9001, ISO 27001, and ISO 27701 standards i.e., in the fields of quality, information security, and privacy of information and always focusing on client satisfaction and integration of QMS, ISMS and PIMS to unique integrated management systems (IMS)

- Establish new roles and responsibilities where every area of RGZ should have staff who are directly responsible for QMS, ISMS and PIMS i.e., quality, information security and privacy-related tasks and maintenance in each department that is capable of performing audits, maintaining documentation, conduct management reviews, and implement any needed changes

- Launch IMS and start to see changes come into action and use a plan to begin putting IMS into action. Monitor process performance and start internal audits to check that all standard requirements are being met

- After the documentation has been prepared and things have started being implemented, conduct internal audit to identify any problems within the scope of IMS based on ISO 9001, ISO 27001, and ISO 27701. Any corrective measures that need to be taken should be taken without any delays. If needed, documentation should be revised. Internal auditors will ensure that all procedures are well implemented, documented, and understood by the staff carrying them out. They will check that the system meets standard requirements, is effective, and is showing improvement

- After internal audit conduct the management review of the progress that IMS based on ISO 9001, ISO 27001 and ISO 27701 is making. This review will help the team identify any underlying issues and the corrective actions that need to be taken to get everything in line with requirements. Management review is a useful tool that will give a precise look at the performance of IMS and any problems that have come about

- The next step but **not covered by this Project** will be assessment and registration by an independent Certification Body for certification of QMS, ISMS and PIMS frameworks based on ISO 9001, ISO 27001, and ISO 27701 standards. The time for RGZ to carry on with the certification process will come and to officially become ISO 9001, ISO/IEC 27001, and ISO/IEC 27701 certified.

The work of the Consultant to be performed to deliver the Integrated Management System (IMS) include **main objectives** as follows:

- Customer satisfaction and deliver products that consistently meet customer requirements and a service that is dependable and can be relied on
- Continual improvement of processes and resulting operational efficiencies
- Internal auditing defined by ISO 9001
- Risk management which means greater consistency and traceability of products and services make problems are easier to avoid and rectify
- Training and Competence
- Brand and Reputation
- Improved the perception of RGZ with staff, customers, and suppliers

- Understood how regulatory requirements impact RGZ and its customers
- Asset protection defined by ISO 27001
- Security policy
- Cyber security strategy and increased attack resilience with ISMS which improved RGZ's ability to prepare for, respond to and recover from any cyber attack
- Incident management
- Threat mitigation that ensured customer records, financial information and intellectual property are protected from loss, theft, and damage through a systematic framework
- Avoided downtime with management of risk, legal compliance and vigilance of future security issues and concerns
- Loss prevention
- Understood how regulatory requirements impact RGZ and its customers, whilst reducing risk of facing prosecution and fines
- Personal data protection
- ISO 27701 enhanced implemented information security management system to address privacy requirements and put in place the systems and infrastructure to support compliance to legislation including ZZPL and GDPR compliance
- ISO 27701 enabled RGZ to assess, react and reduce risks associated with the collection, maintenance and processing of personal information and privacy rights of individuals
- Continued confidentiality
- Data breaches management
- Securing personal information and provided a framework on how to manage and process data and safeguard privacy
- Built customers' trust
- Increased customer satisfaction
- Protected the organization's reputation with ISO 27701 implementation which is a respected standard for privacy information management systems worldwide.

V. WORK PRODUCTS / DELIVERABLES

The products resulting from the work of the Consultant to be performed to deliver the Integrated Management System (IMS) include **main deliverables** as follows:

Phase I:

- Inception report including detailed work and action plan for the individual tasks to be completed.
- GAP analyses and assessment report with relevant recommendations of the current situation of the current system and compare it to the ISO 27001 and ISO 27701 requirements

- Detailed project plan, which includes the identification of individual phases of project implementation with related activities, with a description of the same, as well as a detailed time plan (Gantt chart)

Phase II:

- Documented information required by these standards (e.g., Information Security Policy, BYOD Policy, Mobile Device and Teleworking Policy, Acceptable Use Policy, Email Policy, Internet Acceptable Use Policy, Information Classification Policy, Access Control Policy, Password Policy, Policy on the Use of Encryption, Privacy Policy, Retention of Records, Personal Data Breach, Transfers of Personal Data to Third Countries or International, Data Portability, Managing Subcontract Processing, Complaints, Privacy Notice, Subject Access Request, Data Protection Officer (DPO), etc.) which will be done in cooperation with responsible persons, and their verification will be done at meetings of the IMS Implementation Team.
- Employee training carried out during the ISMS and PIMS implementation process. The training, with the mentioned topics, hours spent and selection of employees, included:
    - Professional training and certification for ISO 27001 Lead Implementer (5 days) and ISO 27701 Lead Implementer (5 days) with international ISO accreditation in accordance with the personal certification model according to the international standard ISO 17024 for a certain number of members of the implementation team - three team members for each standard,
    - Training and certificate of attendance for ISO 27001 and ISO 27701 Internal Auditor of employees (3 days), and especially of the implementation team, in order to become competent internal auditors of ISO standards,
    - General ISO 27001, and ISO 27701 training (1 day) for employees who have a significant impact on information security and protection of personal data.
- The methodology of implementation and application of ISO 27001, and ISO 27701 standards in the RGZ which would be integral. When the complete documentation is completed, the IMS implementation team adopts and, after the verification, releases the documentation for application in accordance with the concept of IMS implementation, and perform the necessary harmonization of implemented management system with the ISMS and PIMS, which includes the design of an integrated IMS.
- Established new roles and responsibilities where every area of RGZ should have staff who are directly responsible for ISMS and PIMS i.e., information security and privacy-related tasks and maintenance in each department that is capable of performing audits, maintaining documentation, conduct management reviews, and implement any needed changes.
- Internal audit prepared and conducted, which includes the initial process of verifying the established ISMS and PIMS compliance in order to identify possible shortcomings and opportunities for improvement. Internal auditors will ensure that all procedures are well implemented, documented, and understood by the staff carrying them out. In order to prepare for certification according to the ISO 27001 and ISO 27701 standards, the Consultant, together with internal auditors from the organization, conduct an internal audit before the certification process, and point out any non-compliance with ISO standards requirements.

Phase III

- Employee training carried out during the QMS implementation process. The training, with the mentioned topics, hours spent and selection of employees, included:
  - Professional training and certification for ISO 9001 Lead Implementer (5 days) with international ISO accreditation in accordance with the personal certification model according to the international standard ISO 17024 for a certain number of members of the implementation team - three team members for this standard,
  - Training and certificate of attendance for ISO 9001 Internal Auditor of employees (3 days), and especially of the implementation team, in order to become competent internal auditors of ISO standard,
  - General ISO 9001 (1 day) for employees who have a significant impact on quality of products and services.
- The methodology of implementation and application of ISO 9001 standard in the RGZ. When the complete documentation is completed, the IMS implementation team adopts and, after the verification, releases the documentation for application in accordance with the concept of IMS implementation, and perform the necessary harmonization of QMS implemented management system with the ISMS and PIMS, which includes the design of an integrated IMS.
- Established new roles and responsibilities where every area of RGZ should have staff who are directly responsible for QMS in each department that is capable of performing audits, maintaining documentation, conduct management reviews, and implement any needed changes.
- Internal audit prepared and conducted, which includes the initial process of verifying the established QMS compliance in order to identify possible shortcomings and opportunities for improvement. Internal auditors will ensure that all procedures are well implemented, documented, and understood by the staff carrying them out. In order to prepare for certification according to the ISO 9001 standard, the Consultant, together with internal auditors from the organization, conduct an internal audit before the certification process, and point out any non-compliance with ISO standard requirement.

Phase IV

- Conducted the management review of the progress that QMS, ISMS and PIMS against ISO 9001, ISO/IEC 27001 and ISO/IEC 27701 was done. This review will help the team identify any underlying issues and the corrective actions that need to be taken to get everything in line with requirements. Management review is a useful tool that will give a precise look at the performance of and any problems that have come about. The IMS system implies the existence of a process of permanent improvement. By reviewing the results of the internal audit by the RGZ's management, this process begins, and key decisions are made regarding the further certification process.

VI. CLIENT'S INPUT

The RGA shall provide Consultant with all the relevant documents required for Integrated Management System (IMS) implementation. RGA shall also provide office space for consultants at the authority premises, assist in data collection and participate in working groups and trainings.

VII. PERIOD OF PERFORMANCE

The work will take place over twelve-months period with the following timeline divided in two phases:

Phase I: Initiation of ISMS and PIMS against ISO/IEC 27001 and ISO/IEC 27701

ISMS/PIMS-15 days after the contract signing: Get Top Management on Board and making sure that the people at the top of RGZ management understand what ISO 27001 and ISO 27701 means for its business because without everyone completely committed it becomes much more difficult to affect change throughout the business

ISMS/PIMS-1 month after the contract signing: Preparation of GAP analyses of the current situation. Once have everyone on board analyze the current system and compare it to the ISO 27001 and ISO 27701 standards

ISMS/PIMS-45 days after the contract signing: Plan everything out for Implementation and having a solid plan in place is essential to making the transition to a new ISMS against ISO 27001 and new PIMS against ISO 27701 standards

ISMS/PIMS-2 months after the contract signing: Decide on an implementation team to begin implementation by top management who should decide on and create an implementation team for ISO 27001 and ISO 27701. This team should be made up of managers from different areas of RGZ business

End of Phase I

Phase II: Implementation of ISMS and PIMS against ISO/IEC 27001 and ISO/IEC 27701

ISMS/PIMS-75 days after the contract signing: Identify core and support processes and map out a plan for meeting ISO 27001 and ISO 27701 standards and be aware of which processes within RGZ coordinate with which requirements

ISMS/PIMS-3 months after the contract signing: Get everyone involved where every single person that works within RGZ should be aware that change is coming with ISO 27001 and ISO 27701

ISMS/PIMS-105 days after the contract signing: Provide employee training, which is crucial to keeping IMS running, and train all of employees on the parts of the system that are specific to their area of work. Training should teach the employees about the procedures that apply to their work, which forms they should be using and how to complete and process them, how to find any specific IMS documented information and how it relates to their position, how to report issues so that they can be fixed, where to find all relevant documents for conducting the internal audits.

Given that training is one of the key activities and considering the importance and role of employee training in the process of introducing ISO standards, attention should be paid to training.

Employee training should be carried out during the ISMS and PIMS implementation process. The training, with the mentioned topics, hours spent and selection of employees, should include:

- Professional training and certification for ISO 27001 Lead Implementer (5 days) and ISO 27701 Lead Implementer (5 days) with international ISO accreditation in accordance with the personal certification model according to the international standard ISO 17024 for a certain number of members of the implementation team - three team members for each standard,

- Training and certificate of attendance for ISO 27001 and ISO 27701 Internal Auditor of employees (3 days), and especially of the implementation team, in order to become competent internal auditors of ISO standards,
- General ISO 27001 and ISO 27701 training (1 day) for employees who have a significant impact on information security and protection of personal data.

ISMS/PIMS-4 months after the contract signing: Identify objectives and responsibilities, develop documented information such as policies, procedures, and instructions with following records within RGZ as an integral part of keeping the business committed to meeting requirements of ISO 27001 and ISO 27701 standards i.e., in the fields of information security and privacy of information

ISMS/PIMS-135 days after the contract signing: Establish new roles and responsibilities where every area of RGZ should have staff who are directly responsible for ISMS and PIMS i.e., information security and privacy-related tasks and maintenance in each department that is capable of performing audits, maintaining documentation, conduct management reviews, and implement any needed changes

ISMS/PIMS-5 months after the contract signing: Launch ISO 27001 and ISO 27701 and start to see changes come into action and use a plan to begin putting these standards into action. Monitor process performance and start internal audits to check that all standard requirements are being met

ISMS/PIMS-165 days after the contract signing: After the documentation has been prepared and things have started being implemented, conduct internal audit to identify any problems within the scope of ISMS and PIMS. Any corrective measures that need to be taken should be taken without any delays. If needed, documentation should be revised. Internal auditors will ensure that all procedures are well implemented, documented, and understood by the staff carrying them out. They will check that the system meets standard requirements, is effective, and is showing improvement

ISMS/PIMS-6 months after the contract signing: After internal audit conduct the management review of the progress that ISMS against ISO 27001 and PIMS against ISO 27701 are making. This review will help the team identify any underlying issues and the corrective actions that need to be taken to get everything in line with requirements. Management review is a useful tool that will give a precise look at the performance of and any problems that have come about.

End of Phase II

Phase III: Implementation of QMS against ISO 9001 and integration in unique IMS

QMS-195 days after the contract signing: Get Top Management on Board and making sure that the people at the top of RGZ management understand what ISO 9001 means for its business because without everyone completely committed it becomes much more difficult to affect change throughout the business

QMS-7 months after the contract signing: Preparation of GAP analyses of the current situation. Once have everyone on board analyze the current system and compare it to the ISO 9001 standard

QMS-225 days after the contract signing: Plan everything out for Implementation and having a solid plan in place is essential to making the transition to a new QMS against ISO 9001 standard

QMS-8 months after the contract signing: Decide on an implementation team to begin implementation by top management who should decide on and create an implementation team for ISO 9001. This team should be made up of managers from different areas of RGZ business

QMS-255 days after the contract signing: Identify core and support processes and map out a plan for meeting ISO 9001 standard and be aware of which processes within RGZ coordinate with which requirements

QMS-9 months after the contract signing: Get everyone involved where every single person that works within RGZ should be aware that change is coming with ISO 9001

QMS-285 days after the contract signing: Provide employee training, which is crucial to keeping IMS running, and train all of employees on the parts of the system that are specific to their area of work. Training should teach the employees about the procedures that apply to their work, which forms they should be using and how to complete and process them, how to find any specific IMS documented information and how it relates to their position, how to report issues so that they can be fixed, where to find all relevant documents for conducting the internal audits.

Given that training is one of the key activities and considering the importance and role of employee training in the process of introducing ISO standards, attention should be paid to training.

Employee training should be carried out during the QMS implementation process. The training, with the mentioned topics, hours spent and selection of employees, should include:

- Professional training and certification for ISO 9001 Lead Implementer (5 days) with international ISO accreditation in accordance with the personal certification model according to the international standard ISO 17024, for a certain number of members of the implementation team - three team members for this standard,
- Training and certificate of attendance for ISO 9001 Internal Auditor of employees (3 days), and especially of the implementation team, in order to become competent internal auditors of ISO 9001 standard,
- General ISO 9001 training (1 day) for employees who have a significant impact on quality of products and services.

QMS-10 months after the contract signing: Identify objectives and responsibilities, develop documented information such as policies, procedures, and instructions with following records within RGZ as an integral part of keeping the business committed to meeting requirements of ISO 9001 standard i.e., in the field of quality of products and services, and always focusing on client satisfaction and integration of QMS with ISMS and PIMS to unique integrated management systems (IMS)

QMS-315 days after the contract signing: Establish new roles and responsibilities where every area of RGZ should have staff who are directly responsible for QMS and quality of products and services tasks and maintenance in each department that is capable of performing audits, maintaining documentation, conduct management reviews, and implement any needed changes.

<u>End of Phase III</u>

Phase IV: Conducting of Internal Audit and Management Review

QMS-11 months after the contract signing: Launch QMS and unique IMS and start to see changes come into action and use a plan to begin putting IMS into action. Monitor process performance and start internal audits to check that all standard requirements are being met

QMS-345 days after the contract signing: After the documentation has been prepared and things have started being implemented, conduct internal audit to identify any problems within the scope of QMS. Any corrective measures that need to be taken should be taken without any delays. If needed, documentation should be revised. Internal auditors will ensure that all procedures are well implemented, documented, and understood by the staff carrying them out. They will check that the system meets standard requirements, is effective, and is showing improvement

QMS-12 months after the contract signing: After internal audit conduct the management review of the progress that QMS against ISO 9001 and IMS are making. This review will help the team identify any underlying issues and the corrective actions that need to be taken to get everything in line with requirements. Management review is a useful tool that will give a precise look at the performance of and any problems that have come about.

End of Phase IV

End of the Project

VIII. PROFESSIONAL QUALIFICATION FOR A CONSULTANT AND REQUIRED TEAM OF EXPERTS

A consultant company, as a part of their technical proposal, will submit the following information:

a) Company Profile and experience highlighting its relevance to the assignment

b) CV's of the members of the team of experts

The company must have more than five years of extensive experience in the field of confirmed certifications for implemented and certified following ISO standards: ISO 9001:2015 and ISO 27001:2013.

The consultant should have strong and relevant track record concerning the IT projects with public sector institutions, entailing oversight of implementation of software solutions, staff training and handover.

Partnership certificate or authorization, issued directly by an internationally accredited certification body in accordance with the personal certification model according to the international standard ISO 17024, for the services of conducting training of persons and their professional evaluation and certification, which must be issued to the legal entity of the bidder, and this will be considered as an advantage.

Person in the capacity as a Certified Trainer with a certificate issued by the accredited certification body from the previous item is an advantage.

Experience in Western Balkans countries and Serbia will be considered as an advantage.

Team of Experts to be provided:

a. Expert 1: Project manager for ISO projects, employed or engaged on a part-time basis within the company with eligibility criteria:

Qualifications and skills

- Education: University degree in the field of technical, organizational, or social sciences
- Strong oral and written English communication skills
- Good mediation and facilitation skills
- At least 7 years of work experience in the field of ISO standards

Specific professional experience

- Experience in project management related to public administration
- At least 7 years of work experience in the field of information technologies

- Certificate on ISO 9001 Lead Auditor (in accordance with the personal certification accreditation according to the international standard ISO 17024)
- Certificate on ISO/IEC 27001 Lead Auditor (in accordance with the personal certification accreditation according to the international standard ISO 17024)
- Certificate on PMI or Prince2 or ISO 21500 Lead Project Manager (in accordance with the personal certification accreditation according to the international standard ISO 17024) is an advantage
- Certificate on ISO 31000 Lead Risk Manager (in accordance with the personal certification accreditation according to the international standard ISO 17024) is an advantage
- Certificate Six Sigma Green Belt (in accordance with the personal certification accreditation (in accordance with the personal certification accreditation according to the international standard ISO 17024)) is an advantage
- Certificate on ISO/IEC 27032 Lead Auditor (in accordance with the personal certification accreditation according to the international standard ISO 17024) is an advantage
- Certificate on ISO/IEC 27701 Lead Implementer (in accordance with the personal certification accreditation according to the international standard ISO 17024) is an advantage
- Passed professional Public Administration Exam is an advantage
- Working experience in Western Balkans and especially in Serbia is an advantage
- Strong oral and written Serbian communication skills is an advantage

b. **Expert 2: Senior ISO standards specialist**, employed or engaged on a part-time basis within the company with eligibility criteria:

Qualifications and skills

- Education: University degree in the field of technical, organizational, or social sciences
- Strong oral and written English communication skills
- Good mediation and facilitation skills
- At least 5 years of work experience in the field of ISO standards

Specific professional experience

- Experience in projects related to public administration
- At least 5 years of work experience in the field of information technologies
- Certificate on ISO/IEC 9001 Lead Auditor (in accordance with the personal certification accreditation according to the international standard ISO 17024)
- Certificate on ISO/IEC 27001 Lead Auditor (in accordance with the personal certification accreditation according to the international standard ISO 17024)
- Certificate on ISO 22301 Lead Auditor (in accordance with the personal certification accreditation according to the international standard ISO 17024) is an advantage
- Strong work experience in the court witness expertise or IT audits in the field of information technology is an advantage
- Certificate on ISO/IEC 27032 Lead Auditor (in accordance with the personal certification accreditation according to the international standard ISO 17024) is an advantage
- Certificate on ISO 20000 Lead Auditor or a valid certificate on ITIL for IT Service Management (in accordance with the personal certification accreditation according to the international standard ISO 17024) is an advantage
- Working experience in Western Balkans and especially in Serbia is an advantage
- Strong oral and written Serbian communication skills is an advantage

c. **Expert 3: ISO standards specialist for standardization of business processes**, employed or engaged on a part-time basis within the company with eligibility criteria:
Qualifications and skills

- Education: University degree in the field of technical, organizational, or social sciences
- Strong oral and written English communication skills
- Good mediation and facilitation skills
- At least 3 years of work experience in the field of ISO standards

Specific professional experience

- Experience in using professional Business Process Management tools
- At least 3 years of work experience in the field of information technology
- Certificate on ISO 9001 Lead Auditor (in accordance with the personal certification accreditation according to the international standard ISO 17024) is an advantage
- Certificate on ISO/IEC 27001 Lead Auditor (in accordance with the personal certification accreditation according to the international standard ISO 17024) is an advantage
- Working experience in Western Balkans and especially in Serbia is an advantage
- Strong oral and written Serbian communication skills is an advantage

d. **Expert 4: ISO standards specialist for information and cyber security**, employed or engaged on a part-time basis within the company with eligibility criteria:
Qualifications and skills

- Education: University degree in the field of technical, organizational, or social sciences
- Strong oral and written English communication skills
- Good mediation and facilitation skills
- At least 2 years of work experience in the field of cyber security

Specific professional experience

- Experience in projects related to cyber security
- Successfully implemented at least three ISO/IEC 27001 standards in the organization in the last five years is an advantage
- At least 2 years of work experience in the field of information technologies
- Strong work experience in the court witness expertise or IT audits in the field of information technology is an advantage
- Working experience in Western Balkans and especially in Serbia is an advantage
- Strong oral and written Serbian communication skills is an advantage

e. **Expert 5: ISO standards specialist for personal data protection**, employed or engaged on a part-time basis within the company with eligibility criteria:
Qualifications and skills

- Education: University degree in the field of law sciences
- Strong oral and written English communication skills
- Good mediation and facilitation skills
- At least 2 years of work experience related to legal expertise in data protection contracts and making organization GDPR compliant

Specific professional experience

- Experience in projects related to drafting internal procedures
- Experience in keeping the business up to date with legal requirements
- Working experience in Western Balkans and especially in Serbia is an advantage
- Strong oral and written Serbian communication skills is an advantage