# Section 7. Terms of Reference

**for**

**Implementation of SO/IEC 42001:2023 - AI management systems**

**Enabling Digital Governance in Serbia (P164824)**

1. **Background Information**

Digitalization is increasingly becoming the backbone of any and all functional restructuring in the public sector, an objective driver of change management and a precondition for transformative development. Going digital, being a horizontal measure, is also accelerating the attainment of Sustainable Development Goals, in further text, SDG. While it directly falls under SDG 16, e-governance is contributing to building stronger institutions – effective, accountable and transparent – at all levels.

The Government of Serbia, elected in June 2017, has heavily prioritized digital transformation of the national economy and state administration. The Prime Minister's Keynote Address before the Parliament stressed digitalization and education as the most important catalysts of innovations, competitiveness and growth for Serbia in the coming years. It also stressed the need for a rapid digitalization of public administration and provision of integrated, secure and citizen-focused electronic services. This political support has materialized in August 2017, when the new Government formed the OITeG and appointed the Prime Minister as head of the Council for Innovative Entrepreneurship and Information Technologies (IT Council).

In addition, the Government of Serbia has requested assistance of the World Bank in supporting the reform efforts, through a loan. To this effect, the World Bank has initiated the Enabling Digital Governance Project (EDGE). The project, expected to be launched in April 2019, aims at contributing to development of the digitalization in Serbia, through implementation of the following components:

*Component 1: Foundations for Digital Service Delivery[[1]](#footnote-2)*

The objective of this component is to establish the necessary cross-cutting foundations to support the use of ICTs in the provision of public services to citizens, and businesses, including inter alia, regulations, standards, and digital infrastructure.

*Component 2. Transforming Services for Citizens, Business and Government*

The objective of this component is to support re-engineering, digitalization, and piloting of selected administrative e-services. It will support improvements in back-office processes to reduce administrative burdens and increase efficiency of administrative service delivery to citizens and businesses.

*Component 3.* *Digital Skills Development, Institutional Strengthening and Change Management*

Activities under this component will focus on transforming the provision of administrative services to citizens and businesses, which will result in the change of the way public servants do their work as well as the way citizens and businesses interact with the administration. The key result of this component is enhanced capacity for project management and institutional coordination to achieve project results. This component will include strategic frameworks to help all stakeholders to understand, commit and successfully develop digital skills, implement change and, by promoting digital skills and changes, contribute to further institutional strengthening which will bring major benefits to citizens and business.

For the purposes of effectively managing and coordinating EDGe and future projects with IFI financing, the Project Implementation Unit (PIU) has been founded at the OITeG. PIU will have a dedicated staff to coordinate and supervise implementation of here requested activity.

1. **Objective**

The objective of this engagement is to support the Government of Serbia in establishing a robust, ethical, and legally compliant framework for managing Artificial Intelligence (AI) systems in public administration. This includes aligning organizational practices with the ISO/IEC 42001 standard on AI Management Systems, strengthening institutional capacity through tailored training and policy development, and preparing for potential certification. The ultimate goal is to ensure responsible, transparent, and risk-aware use of AI that upholds public trust and safeguards individual rights.

1. **Scope of Work**

The assignment will be implemented in two phases:

**Phase I – Development of AI Management Framework and Training Curricula**

* Conduct situational analysis and gap assessment regarding AI usage in public administration;
* Develop and/or update training curricula in line with ISO/IEC 42001 requirements;
* Draft policies and procedures for AI risk management, legal compliance, and governance;
* Define institutional roles and responsibilities related to AI system oversight;
* Develop tailored training and awareness materials for managers, IT, legal, and executive staff;
* Prepare Guidelines for implementation of ISO/IEC 42001 in public administration.

**Phase II – Training Delivery and Certification Readiness**

* Deliver in-person and hybrid training for key staff;
* Conduct internal audit of the AI management system;
* Support certification preparation and selection of a certification body;
* Develop sustainability recommendations and roadmap for long-term adoption of AIMS.

**Progress Reporting**

In addition to activities covered under the three phases as described above, the Consultant firm must also submit quarterly progress reports (once every three months) detailing activities completed in the quarter being reported on with respect to activities planned in the Inception Report. Reasons for delay or slippage, if any, must also be presented along with explanation why the delay occurred and description which actions should be taken so the total timeframe of the project remains the same.

On completion of all activities envisaged under the assignment, the consultant firm shall submit a Final Report that should contain a summarized description of activities the Consultant firm carried out over the assignment period and the results achieved during the development and implementation of the Data protection officer trainings and awareness raising trainings.

The Final Report and the quarterly progress reports must be submitted to the PIU within OITeG. The Final Report must be submitted one month prior to the completion of the contract.

1. **Timeframe and duration**

The project will span over **6 (six) months**

1. **Deliverables, Timelines**

|  |  |  |
| --- | --- | --- |
| **No.** | ***Deliverable*** | ***Deadline*** |
| 1 | Situational analysis and risk assessment report | 1 month after contract signing |
| 2 | Inception Report with updated training curricula and implementation roadmap | 2 month after contract signing |
| 3 | Draft and final Guidelines for AIMS in public administration | 4 months after contract signing |
| 4 | Report on completed in-person training sessions | 4 months after contract signing |
| 5 | Internal audit report and certification readiness recommendations | 5 months after contract signing |
| 7 | Final Report | 6 months after contract signing |

1. **Consultant Qualifications**

In order to be selected, the Consultant firm must possess, at the minimum, the following qualifications:

1. The Consultant firm must prove its capability by listing its experience in the last five (5) years (2019-2024) related to: minimum 2 projects, where the assignment, or a part thereof, was dedicated to implementation of system management (ISO 42001, ISO 27001, or similar)
2. Demonstrated experience in delivering training and capacity building for public sector entities is a plus;
3. Proven experience of EU and Serbian legislation relevant to data protection, AI, and information security.
4. **Team requirements**

**Key expert 1: Team Leader**

* Minimum fifteen (15) years of general working experience.
* Minimum Bachelor’s degree in the field of engineering or organizational sciences, IT or similar.
* At least ten (10) years of professional experience on leadership positions.
* Proven record of leading capacity building projects in the public sector.
* Participation in a Team Leader role (or in any other leadership/key expert role) on at least one (1) project financed by IFIs, donors and/or respective governments.
* Participation in implementation or GAP analysis for ISO 27001 in at least ten (10) public administration (PA) organizations.
* Experience in applying ISO 27001 principles as a basis for AI-related risk identification and mitigation (e.g. data protection, incident response, risk management, secure training data and outputs).
* Experience in supporting responsible and trustworthy AI through structured management system approaches.
* Certified as:
  + Lead Auditor - ISO/IEC 42001 (Artificial intelligence — Management system),
  + Lead Implementer for ISO/IEC 42001 (AI management systems),
  + Lead Implementer for information security management system - ISO/IEC 27001:2022 is an advantage,
  + Lead Auditor for information security management system - ISO/IEC 27001:2022 is an advantage,
  + Lead Implementer for privacy information management system - ISO/IEC 27701:2019 is an advantage.
* Experience as a Lead Auditor at accredited certification bodies (accredited by IAF members) for the following standards is an advantage:
  + ISO/IEC 27001 - Information security, cybersecurity and privacy protection — Information security management systems,
  + ISO/IEC 27701 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management,
  + ISO/IEC 27017 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services,
  + ISO/IEC 27018 - Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
* Excellent communication, organization, and teamwork skills.
* Excellent English written and presentation skills.

Key expert 2: AI expert

* Minimum ten (10) years of general working experience.
* Minimum Bachelor’s degree in the field of organizational sciences, IT or similar.
* Proven track record in leading the development and/or delivering online training programs.
* Certified as:
  + Lead Auditor - ISO/IEC 42001 (Artificial intelligence — Management system),
  + Lead Implementer for information technology, artificial intelligence Management system - ISO/IEC 42001,
  + Lead Implementer for information security management system - ISO/IEC 27001:2022 is an advantage,
  + Lead Auditor for information security management system - ISO/IEC 27001:2022 is an advantage,
  + Lead Implementer for privacy information management system - ISO/IEC 27701:2019 is an advantage.
* Proven experience in developing or reviewing AI governance structures and risk mitigation approaches in line with ISO 42001 requirements.
* Experience in integrating ISO/IEC 42001 with existing management system standards (e.g. ISO/IEC 27001, ISO/IEC 9001, ISO/IEC 27701).
* Excellent communication, organization and teamwork skills.
* Excellent English written and presentation skills.

Key expert 3: Project Coordinator

* Minimum fifteen (15) years of general working experience.
* Minimum Bachelor’s degree in the field of organizational or social sciences, IT or similar.
* Minimum ten (10) years of working experience on leadership and/or Project Coordinator positions.
* Participation in Project Coordinator role on at least one (1) project financed by IFIs, donors and/or respective governments is an advantage..
* Understanding of ISO standards implementation processes, including coordination of expert teams and alignment with institutional procedures.
* Excellent English speaking, written and presentation skills.

Non key expert: Provisional implementer

* Minimum five (5) years of general working experience.
* Minimum Bachelor’s degree in the field of organizational or social sciences, IT or similar
* Understanding of ISO standards implementation processes, including coordination of expert teams and alignment with institutional procedures.
* Excellent English speaking, written and presentation skills.

1. **Evaluation**

The Consultant which obtains the highest score during evaluation of expressions of interest will be invited to submit technical and financial proposals.

1. Under subcomponent 1.4 in Project Appraisal Document of the Project is emphasized the importance to implement the activities, which will ensure compliance with the General Data Protection Regulation (GDPR) and Law on Personal Data Protection, as well as Cybersecurity activities, which will ensure compliance with Law on Information Security [↑](#footnote-ref-2)