

Modernization of Government Services Project

Project ID No. P148537

Terms of Reference

Consulting services to develop standards and procedures related to cyber security for Government Private Cloud Computing Platform and IT Management of the Government IT Infrastructure

I. Background

Country background

The Government of Moldova is determined to fundamentally change the way how public services are provided in Moldova through a variety of interventions for modernization of service delivery, which combat corruption, foster a customer care culture, enhance access, as well as increases efficiency in the Moldovan public administration.

Therefore, the one of the main objectives of the Administration Reform Strategy 2016-2020 and Government's working program for years 2016-2018 is the modernization of the public services.

Moldova has made considerable progress both in terms of public administration reform, exceeding by indicators average of countries in Europe and Central Asia and countries with middle and low income, as well as the size Government modernization using information and communication technology (ICT), the Government of creating a world-class ICT infrastructure that allows the development and supply of electronic services to the highest quality standards.

Current situation in the sector

Even though some progress has been made over the last decade, citizens still view corruption as a significant problem. While business process and e-governance reform efforts have somewhat improved business services, such measures have not yet been applied to administrative services.

Businesses and citizens continue to face many constraints in the interaction with the state, one of the most important is corruption perceived by 40 percent of companies as a major impediment to business (according to the World Bank, EBRD Business Environment and Enterprise Performance Survey (2013). Institutional reforms aimed at reducing corruption are also at the forefront of the EU's requirements for Moldova's progress. The most important challenges ahead are strengthening the rule of law, reforms in the public administration, including professionalism and anti-corruption efforts and improving competitiveness and the business environment.

Although the Government has launched the reform of public services in 2014-2016 and has committed to digitize and provide online access to all public services by 2020, lack of capacity and expertise to perform reengineering and process optimization remains a problem that prevents achieving this.

Also, there is room for rationalization to over 580 existing public service by withdrawing from use the obsolete services.

To meet these challenges, the Government, in accordance with the Public Administration Reform Strategy for the years 2016-2020 (especially the component "Modernization of Public Services") plans a major transformation exercise (qualitative and quantitative) of administrative public services, provided by central public administration authorities through: a) removing outdated public services or merging several services in one; b) increased access to local public services through various channels; c) reducing the number of documents required for public services, and the service delivery time; e) ensuring a high level of satisfaction with the quality of government service delivery.

The Government services are highly depending on IT infrastructure by which the services are delivered and consumed. The Government Private Cloud Platform (MCloud) is the heart of this infrastructure.

Officially launched in 2013, MCloud is currently used by most of Government Agencies to provide G2B and G2C electronic services. To respond to security challenges which was posed by implementation of a Government Private Cloud Platform, the MCloud Security Architecture document was developed and approved in 2014 which define the security requirements to be implemented starting with the physical level up to application one for different type of MCloud services - IaaS, PaaS, SaaS. Meanwhile the MCloud has undergone architectural and technological changes which requires to review and adjust the MCloud security requirements to new realities.

At the same time, in the context the reorganization initiatives, implemented by the Government of Moldova, regarding how IT services are provided and managed in Government Sector requires a review on how IT process are organized as well how cyber security is ensured by the Government IT platforms.

The Government of Moldova has requested the World Bank's assistance for a Public Administration Reform (PAR) operation, planned for delivery commencing in FY17 to 2021 (Modernization of Government Services Project –MGSP). Major results of the operation include better quality, accessibility, and increased efficiency of selected government administrative services.

II. Objective of the Assignment

The purpose of this assignment is to develop the Cyber Security Controls to be applied at Government Private Cloud Infrastructure level and IT Infrastructure Management standards and procedures to be used by the Government Authorities to manage and secure their IT infrastructure.

III. Scope of work

The qualified consulting firm (herein after referred to as – the Consultant) is expected to:

1. Strengthening government capability to ensure proper cyber security of the MCloud.

- 1.1. Perform a review of current state of the Government Private Cloud Platform (MCloud) security, including the status of implementation of MCloud Security Architecture document (Executive Order of the Government General Secretary Nr. 380 from 03.11.2014).
- 1.2. Develop a next version of the detailed cyber security and operation controls to be applied for MCloud which should:
 - 1.2.1. be based on latest version of Center of Internet Security (CIS) cyber security controls, ISO 27001/ISO27002, OWASP application security best practices;
 - 1.2.2. take into consideration the security requirements defined in Government Decision nr.1123 on personal data protection and Government Decision nr. 203 on minimal cyber security requirements
 - 1.2.3. define the controls to be applied as by cloud service provider for IaaS, PaaS and SaaS services as well by the MCloud service consumers up to end user to ensure a secure ecosystem of government IT services;
 - 1.2.4. be relevant for both: private cloud model (all information systems are deployed in MCloud), as well as, for hybrid cloud model (some systems are deployed on in-house infrastructure and other on MCloud, as well some systems are deployed in MCloud and other in public Cloud);

- 1.2.5. define different security levels based on the impact of the system in the government information ecosystem.
- 1.2.6. ensure the security baseline required to protect the government IT Services.
- 1.3. Develop a guideline how to implement the defined controls;
- 1.4. Develop recommendations regarding required amendments to legal framework to sustain the adoption and implementation;
- 1.5. Perform one training session for up to 20 IT and Information Security employees of the government agencies that will pilot the implementing the defined controls.
- 1.6. Develop on-line training module to be delivered using e-Learning System;
- Note:** The number of piloting agencies will not exceed four.
- 1.7. Organize one workshops for up to 50 representatives of public service providers to present the results of the defined security controls and the implementation guidelines.

2. Preparing Standards and procedures for IT management

- 2.1. Perform a review of current IT management process and standard applied by the piloting government agencies;

Note: The number of piloting agencies will not exceed four.

- 2.2. Develop IT management standards and procedures to be applied by government authorities for managing the information systems and infrastructure. The developed standards and procedure should:
 - 1.2.1. be based on ITIL and COBIT best practices and integrate the relevant requirements from ISO 27001 and ISO 9001 standards;
 - 1.2.2. integrate the relevant practices from DevOps and Agile Service Management approach to deliver IT Services;
 - 1.2.3. be applied to the outsourcing and in-house IT service management scenarios;
 - 1.2.4. take into consideration the private and hybrid cloud operation;
 - 1.2.5. Intergrade the controls defined in section 1 “Strengthening government capability to ensure proper cyber security of the cloud”.
- 2.3. Perform one training session for up to 20 IT and Information Security employees of the government agencies that will pilot the implementation of process and procedure;
- 2.4. Develop on-line training module to be delivered using e-Learning System;
- 2.5. Organize a workshop for up to 50 representatives of public service providers to present the results of the assignment, including developed procedures and standards.
- 2.6. Develop recommendations regarding required amendments to legal framework as necessary.

To fulfill the tasks the Consultant shall conduct on-site assessments, interviews with the responsible public servants, beneficiaries and other relevant stakeholders to collect information and understand the public services under investigation.

IV. Timing

The Consultant is expected to complete the assignment in 10 months from the contract signature.

V. Deliverables and Schedule of Deliverables

The list of deliverables and the deliverables schedule are presented below. All deliverables should be provided in hard copy and electronic format in Romanian language.

1. Strengthening government capability to ensure proper cyber security of the cloud.

#	Deliverables	Schedule from the assignment start date
1	The report regarding status of implementation of MCloud Security Architecture, including the proposal for next version of the cloud security and operation controls	4 weeks
2	MCloud cyber security and operation controls document	28 weeks
3	MCloud cyber security and operation controls implementation guideline	30 weeks
4	Report which will include the recommendations regarding required amendments to legal framework, including improvement of the current agreements/contracts	28 weeks
5	Training for representative of the piloting government agencies, including the training materials	32 weeks
6	Workshop for public service providers	32weeks
7	On-line training modules for Moodle e-Learning System which cover the developed MCloud cyber security and operation controls and guidelines to be delivered.	34 weeks

2. IT Management standards and procedures.

#	Deliverables	Deadlines from the assignment start date
1	The report on the status of current IT management and IT infrastructure processes and standards, which will include recommendations on processes and procedures to be developed and implement, processes and procedure implementation planed	9 weeks
2	Developed and documented IT infrastructure procedures and standards	32 weeks
3	Implementation training for representative of the piloting government agencies, including the training materials	34 weeks
4	Report which will include the recommendations regarding required amendments to legal framework	34 weeks
5	Presentation workshop for public services providers	35 weeks
6	On-line training modules for Moodle e-Learning System which cover the developed IT Management standards and procedures.	36 weeks

--	--	--

VI. Reporting requirements

The Consultant shall work under the general supervision of the e-Governance Agency's Director, who will facilitate the Consultant's access to the necessary documents, materials and key stakeholders to the assignment. The Consultant shall also coordinate the work with the Quality Assurance and Security Expert of the e-Governance Agency.

VII. Resources

The e-Governance Agency will provide the Consultant with the core data on the institutions under the scope of the assignment and other available information on public services; will facilitate the interaction with appropriate institutions, offices and make the necessary arrangements for consultations with relevant stakeholders.

VIII. Consultant's qualification and experience

The Consultant should be a firm with extensive local and international experience in the field of IT and Cyber security consultancy, which shall have:

- Professional experience in providing consultancy, including development of cyber security process and procedures in area of IT Service Management and Cyber Security controls (during the last 5 years);
- Minimum one successful project in the last three years per each of the following areas:
 - IT Service Management Implementation;
 - Cyber Security Controls, including in cloud environment, development and implementation;
- Certification obtained related to quality and security management (ISO 9001, ISO 27001) would be an asset;

Key experts

Key experts have a crucial role in implementing the contract. These terms of reference contain the required key experts' profiles. The Consultant shall submit CVs and Statements of Exclusivity and Availability for the following key experts:

- Key Expert 1: Team leader
- Key Expert 2: IT Service Management Expert
- Key Expert 3: Cyber Security Expert
- Key Expert 4: Legal expert
- Key Expert 5: e-Learning content developer

Key expert 1: Team Leader

The Team Leader is responsible for the day-to-day liaison with the Contracting Authority; s/he must ensure the internal coordination and guidance of all experts of the project and coordination of the project with external counterparts.

The Team Leader must also ensure availability of suitable experts in accordance with the Project Work Plan.

The Team Leader shall oversee that all deliverables and reporting obligations are fulfilled in a timely manner to a high-quality standard.

Qualifications and skills

- University degree in areas such as computer sciences, engineering, and telecommunications or related;
- Minimum 5 years of experience in area of IT Service Management and Information Security Management;
- Excellent understanding of DevOps, Agile Service Management, Cloud Computing Operation aspects;
- Excellent understanding of internationally recognized standards and best practices (e.g., ITIL, COBIT, CIS Controls, OWASP, ISO/IEC 270002, etc.)
- Proved professional experience in providing the trainings and workshops in IT and/or Information Security areas; At least 3 years of experience in project management in public or private sectors;
- Certifications in ITIL (at least ITIL Foundation Level) and security qualifications such as CISM, CISSP and/or CEH are a plus;
- Ability to effectively communicate and write in Romanian and/or English. Knowledge of Russian is an advantage.

Key expert 2: IT Service Management Expert

The IT Service Management expert is responsible for defining the process related to IT Service Management and developing the required IT Service Management procedures and standards, including MCloud operation controls.

Qualifications and skills

- University degree in areas such as computer sciences, engineering, and telecommunications or related;
- Minimum 5 years of experience in area of IT Service Management consultancy;
- Proven experience in the following capability areas:
 - IT Operating Model: Accessing and developing IT operating models s. Hands on experience, or familiarity with the various capability components of an IT function
 - IT Service Management: Detailed experience of assessing, designing and implementing IT processes and procedures in the areas of Service Management, Software Delivery, Vendor Management, and Governance
- Demonstrated extensive knowledge of DevOps, Agile Service Management and Private and Hybrid Cloud Operation aspects, internationally recognized standards and best practices (e.g., ITIL, COBIT, CIS Controls, ISO/IEC 270002, etc.);
- Proved professional experience in providing the trainings and workshops in IT management and operation area;
- Certifications in ITIL (at least ITIL Practitioner Level) are a plus;
- Experience in working with governmental organizations would be an asset;
- Ability to effectively communicate and write in Romanian and/or English. Knowledge of Russian is an advantage.

Key expert 3: Cyber Security Expert

The Cyber Security Expert is responsible for and developing the required cyber security procedures related to IT Service and defining the next version of MCloud cyber security controls.

Qualifications and skills

- University degree in areas such as computer sciences, engineering, and telecommunications or related;
- Minimum 5 years of experience in area of Information/Cyber Security consultancy;
- Proven experience in the following capability areas:
 - Cloud Security: experience in developing/implementing the security controls for private or hybrid cloud deployment models.
 - Information/Cyber Security Operations: experience of designing and implementing information/cyber security operation process and procedures related to IT Infrastructure. Experience in implementing and managing a cloud infrastructure will be considered a plus.
- Excellent understanding of internationally recognized standards and best practices (e.g., ITIL, COBIT, CIS Controls, ISO/IEC 270002, etc.);
- Demonstrated extensive knowledge of Private and Hybrid Cloud Operation aspects;
- Proved professional experience in providing the trainings and workshops in Information and Cyber Security area;
- Certifications such as CISM, CISSP and/or CCSP are a plus;
- Experience in working with governmental organizations would be an asset;
- Ability to effectively communicate and write in Romanian and/or English. Knowledge of Russian is an advantage.

Key expert 4: Legal Expert

The Legal Expert is responsible for all legal-related tasks included in this project.

Qualifications and skills

- University degree or equivalent in Law;
- Minimum three (3) years of experience in legal drafting and conducting Regulatory Impact Assessment, with special reference to the public-sector IT service delivery and/or public institution IT management is required;
- Demonstrated experience in IT and Cyber Security Legal area; Experience in working with governmental organizations would be an asset;
- Fluency in Romanian, both written and spoken, knowledge of English language will be a strong asset;
- Computer literate.

Key expert 5: e-Learning content developer

- University degree in areas such as Computer Sciences or related field;
- At least 3 years of experience in developing of training modules using e-learning platforms;
- Minimum one successful training modules developed and provided using e-learning platform based on Moodle;
- Ability to effectively communicate and write in Romanian;
- Certifications in Moodle training is an asset.