Modernization of Government Services Project

Project ID No. P148537

Terms of Reference
Consulting Services for Developing e-learning Module for Cyber Security Training

I. Background

From 2006 to 2013, Moldova modernized its civil service legislation and administrative processes under the Central Public Administration Reform (CPAR), supported by the Bank's administered CPAR MDTF. However, additional efforts are needed to transform Moldova public administration and bring it closer to the EU standards as planned under the Action Plan for implementation of the Association Agreement with the EU, signed in 2014.

Governance is identified as a cross-cutting issue and interventions are planned to improve the business enabling environment, enhance public administration reform and quality of public service delivery. The Government has requested the World Bank's assistance for a PAR operation, planned for delivery commencing in financial year 2018 to 2023, called Modernization of Government Services Project (further MGSP, or the Project).

The design of the Project takes into account the Government of Moldova vision, stated in the Public Administration Reform Strategy 2016-2020, relies on the Government Services Modernization Action Plan for 2017-2021 and makes extensive use of institutional and technological achievements of Governance e-Transformation Project (GeT) implemented by the Government of Moldova and World Bank until 2016.

The project objective to achieve improvements in access, efficiency and quality of delivery of selected administrative services is planned to be fulfilled through the following four components:

1. Public Service Modernization

The key activities under this component focus on re-engineering a group of government to citizen and government to business administrative services, piloting of one-stop-shops for public service delivery in selected locations and explore the possibility of rolling out at national level; increased awareness of citizens on public services and availability of e-services.

2. Aligning institutional capabilities to new model of service delivery

The objective of this Component is to ensure that the institutional capabilities of key government agencies are aligned with and support the new model of public services delivery. Technical assistance will be provided to all institutions responsible for the delivery of public services re-engineered and digitized under MGSP, as well as partner entities participating in Centers for Unified Public Services (CUPS) pilots. The Component will also address the capabilities of structural units in the government responsible for public services modernization reform management and coordination. Specifically, Component 3 of the MGSP supports the adjustment of institutional and staff capacities of key Government agencies to the new citizen-centric model and digital administrative service delivery arrangements.

3. Digital Platform and Services

The main objective of this component is to digitize selected re-engineered government services; complete and strengthen a common infrastructure and mechanisms for rapid deployment of ICT-enabled public services; introduce government wide IT Management and Cyber Security standards and procedures.

Adoption of Cyber Security standards, policies and processes, requires to review the standard approach to capacity building, used in the Government Agencies, and introduce a new approach based on to training using e-learning platforms. Classroom trainings are expensive, time-consuming, and the results are not long lasting due to high turnover of IT staff and emergence of new technologies. The development and use of an e-learning

security training modules with a set of video courses is an efficient way to decrease training costs and increase the total number of trainees, while maintaining an adequate level of efficiency and quality of training, encompassing general security awareness raising for public employees and targeted security trainings required for IT staff.

I. Objectives

The primary objective of the assignment is to develop Moodle e-learning modules for different categories of roles in public institutions (Managers, Users, IT Administrators, Developers) in order to:

- Build the basic knowledge and skills in area of information and cyber security principles and best practices within Government Authorities;
- Create a security culture across Government Authorities and keep on reminding employees about its importance and their contribution in that.

II. Scope of Work

The assignment covers the following areas of activity:

1. Develop and integrate in Moodle e-learning system, managed by the e-Governance Agency, of the following modules related to cyber and information security:

1.1. General Security Awareness training course intended for all Government Authorities employees to teach them the fundamentals of security and security best practices. The training course should cover the following topics:

1) Introduction in Security Governance Framework;
2) Users responsibilities regarding security (cyber and information);
3) Web and Cyber Threats;
4) Social Engineering;
5) Phishing protection;
6) Passwords Security;
7) Email Security;
8) Malware Protection;
9) Identity Theft;
10) Browsing the Web Securely;
11) Safe Internet Practices;
12) The Clean Desk Principle;
13) Physical Security;
14) Access Control;
15) Working Remotely Safely;
16) Intellectual Property;
17) Privacy;
18) Social Networks security;
19) The Bring Your Own Device concept;
20) Smartphones security;
21) Mobiles Devices security;
22) Traveling Securely;

1.2. Managers Security Awareness training course intended for Government Authorities Managers to teach the managers' roles and responsibilities in ensuring the use of best security practices in the Government Authorities. This training course should cover:

1) Introduction to Information and Cyber Security;
2) Security (cyber and information) Roles and Responsibilities;
3) Components of a Security (cyber and information) Governance Framework;
4) Security (cyber and information) and Information Technology;
5) Security Risks Posed by New Technology and Mobility;
6) The Moldovan legislation regarding Information and Cyber Security.

1.3. IT Administrators Security Awareness training course intended for all Government Authorities IT Administrators and are intended to educate information technology professionals on the importance of security best practices for networks and information systems. This training course should cover:

1) IT Administrator Role and Responsibilities in ensuring organization security;
2) Network and Information System security overview;
3) Common Network and Information System attacks;
4) Best practice in securing Networks and Information System;
5) Best practices in securing Data Repositories.

1.4. Application Developers Security Awareness training course intended for all Government Authorities employees directly or indirectly involved in development of electronic services and are intended to educate information technology professionals on the importance of security best practices in process of the application development. This training course should cover:

1) Application Security Overview;
2) Common Application Attacks;
3) Security in the Application Development process;
4) Cryptography Overview.

2. Each course must contain up to 10 lessons with up to 20 hours duration, that covers all specified themes (topics). Course have to be supported with content and glossary. Each lesson must contain short description of lesson, lesson notes and video lesson (presentation with audio or practical lesson). Each course lesson must contain a question bank that will contain not less than 10 multiple choice questions.
3. For each course, evaluation tests have to be developed. The test must include not less than 20 multiple choice questions selected randomly from question bank.
4. The developed modules together with evaluation tests will be piloted within up to 3 governmental institutions. The training modules and tests will be adjusted based on the feedback received after piloting process.

III. Deliverables and Schedule of Deliverables

The list of deliverables and the delivery schedule are presented below. All deliverables must be provided in Romanian languadge.

#	Deliverables	Schedule from the assignment start date
1	**The report presenting the training course organization structure, including the evaluation tests, and implementation plan**	**2 weeks**
2	**The content proposed to be included in the training courses, including the question banks**	**3 weeks**
2.1	General Security Awareness	3 weeks
2.2	Managers Security Awareness	5 weeks
2.3	IT Administrators Security Awareness	8 weeks
2.4	Application Developers Security Awareness	11 weeks

3.	**Approved training course content, including the question banks and evaluation tests, integrated in the Moodle e-learning system**	**4 weeks**
	General Security Awareness	4 weeks
	Managers Security Awareness	5 weeks
	IT Administrators Security Awareness	6 weeks
	Application Developers Security Awareness	7 weeks
4	**Piloting the training courses and evaluation tests**	**8 weeks**
5	**Updated training courses, including the question banks and evaluation tests, in the Moodle e-learning system, based on the feedback from piloting received during the training piloting**	**12 weeks**

IV. Timing

The assignment is expected to start in **September 2019**. The estimated duration of the contract is 4 months.

V. Institutional Arrangements

Reporting: The Consultant will work under the direct supervision of the Quality Assurance and Security Consultant who will facilitate the Consultant's access to the necessary documents, materials and key stakeholders to the assignment.

VI. Resources

The Moodle e-learning system is installed on MCloud. All necessary access to the Moodle system and Moodle configurations will be provided by the Client according to Consultant's needs.

VII. Qualification requirements

Minimum requirements for the Consultant:

- Professional experience in providing the trainings and workshops in information and cyber security area (during the last 3 years);
- Minimum one successful training project related to information/cyber security which cover the security aspect at user, management and IT level in the last 3 years;
- Demonstrated experience in developing the e-learning modules in the area of information/cyber security;
- Experience in working with governmental organizations would be an asset.

Key Staff

The Consultant shall provide the following key experts with the proven qualifications:

- Key expert 1: e-Learning Platform Engineer
- Key expert 2: e-Learning Content Developer

The minimum qualification requirements for the key staff members are described below:

Key expert 1: e-Learning Platform Engineer

- University degree in areas such as Computer Sciences or related field;

- Proved professional experience in area of system installation and administration;
- At least three years of experience in administration of the Moodle e-learning platform;
- Minimum one successful project in the last three years in installation and configuration of e-learning training modules in the Moodle e-learning platform;
- Ability to effectively communicate and write in Romanian.

Key expert 2: e-Learning content developer

- University degree in areas such as Computer Sciences or related field;
- Proved professional experience in providing the trainings and workshops in information and cyber security area;
- At least one 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;
- Excellent understanding of internationally recognized standards and best practices (e.g. OWASP, ISO/IEC 270002, etc.);
- Ability to effectively communicate and write in Romanian;
- Certifications in Moodle training is an asset.