Information Security Management System (ISMS) management solution

1. Background and purpose

The purpose of the subject Request for Proposals (RFP) to solicit proposals for the provision of Secure Information Security Management System (ISMS) integrated enterprise management solution for a public entity, Georgia Revenue Service that is currently implementing information security ISO 27001 standard.
The solution shall manage policies of ISO 27001 IT controls and risk information throughout the organization and create continuous compliance by automating risk management and PLAN-DO-CHECK-ACT processes in an ISMS as defined in ISO 27001.

The ISMS solution shall provide a framework for bringing together ISO 27001 policies, procedures, metrics, controls, and risks.

The solution shall also cover the main requirements of the data protection regulation per General Data Protection Regulation (GDPR) and optionally offer Business Continuity Planning (BCP) management module.

The objective of the integration of the ISMS platform is to systemize IT and information security throughout the organization, provide an overview through a complete mapping of information assets, develop a comprehensive plan with controls and actions, have a tool for risk management and risk assessment, and maintain continuous governance of the ISO 27001 control objectives.

2. Solution Description and Requirements

The proposed ISMS solution shall represent a comprehensive unified platform to ensure the organization's compliance with the ISO 27001 standard, as well as cover GDPR and optionally BCP activities.
The ISMS solution must provide a platform to gather organization's all compliance efforts (including GDPR) while clearly documenting and demonstrating organization's compliance with the ISO 27001 standard and the 114 control objectives of Annex A of the standard. The solution shall allow for possibility to associate the objective of the management system with performance metrics to ensure that ISO 27001 certification is maintained once it is achieved.

General Requirements of the ISMS platform

Overall the comprehensive ISMS platform shall include:

- Complete overview of all phases of the compliance program
- Policy and BCP Templates for all ISO 27001 tasks (and GDPR tasks)
- Policy Management and Compliance
- Risk Management module with readymade threat catalogue
- Time estimates for all major milestones and final project

- Overview of assigned tasks
- Data Protection mangement (GDPR) module
- Automatic measurement of organization’s compliance readienss
- Business continuity management module, optionally
- Awareness activity and testing management
- Clear and concise visual reporting/dashboards.

Detailed Requirements

Support Standard and Regulatory Compliance
The prospective ISMS solution must effectively support compliance with the rules and regulations of the ISO 27001 Standard and GDPR. The solution must provide possibility to upload regulatory and legislative documents directly into the ISMS, mapping each article of the applicable regulation to the corresponding policy and/or procedure that ensures compliance. This solution feature should allow for a built-in compliance checklist within the ISMS system that is easy to review and audit for completeness.

Risk Assessment Functionality
As effective risk assessment is a crucial and integral part of any ISMS solution, the prospective solution must allow for an ability to create a comprehensive threat catalogue and have quantified risk management functionality. The solution must provide an ability to calculate risk scores or assign them using pre-existing and consistent criteria. The solution must have visual representation of the overall risk standing of an organization at any given time and ability to recalibrate.

The solution must allow users to create and assign security classifications to different configurations items or supporting services that are registered in the system, giving an organization better oversight of the highest-vulnerability vectors for a data breach.

Audit Process Facilitation
As the organization for which ISMS solution is to be procured will be seeking compliance with the ISO 27001 standard, internal and external audits (including re-certification audits) will constitute a regular activity for the organization. The ISMS solution must include integrated tools that facilitate the audit process and allow for upload of regulatory documents directly into the system and map the requirements to the corresponding controls.

GDPR Support
Prospective ISMS solution must offer visibility into GDPR management, especially in terms of managing data requests from data subjects.

Dashboard and Reporting
The proposed ISMS solution must offer a clear and simple dashboard system, where both solution users and executive managers can easily navigate and view all compliance actions, status, threats and risk standing, offering real-time insight into the functioning and overall state of the ISMS in the organization. The solution

shall have a capability to demonstrate clearly the scope and compliance of ISMS program during the ISO 27001 Certification Audit with a Statement of Applicability on a single page.

3. Technical Specifications

The proposed ISMS solution may be either On-Premise or Software as a Service (SaaS), housed on a secure well-known platform.

The ISMS solution shall provide capability for up to 1500 end users (with the possibility of expansion) and 2 administrative users.

The proposal shall include price for 5-year subscription, with the possibility of an advance payment option in full.

4. Installation, Support and Upgrades

The prospective contractor shall install or actively participate hands-on in the installation and rollout process of the ISMS solution for the company.

The prospective ISMS solution provider shall ensure access to technical support and regular upgrades for the standard solution and or included modules covered by the contract.

Technical support shall be available through online ticketing systems, mail or telephone. Technical support stipulated under the prospective contract shall include specific SLA.

The end user of ISMS solution is Georgian Revenue Service.

5. Additional information

The prospective contractor shall outline any additional or extra services potentially offered along with the requested solution or any other services that potentially may be of interest to the organization in the final offer.