Terms of Reference

Serbia

Tax Administration Modernization Project (TAMP)

Security Audit Of The STA IT Systems

Background

The TAMP is a five-year project starting in 2019, funded through a World Bank loan to the Government of Serbia, which has as its primary objective to contribute to the achievement of STA's future vision: to become an organization characterized by paperless operations, a taxpayer-friendly administration providing world-class services, equipped with sharp, ICT-enabled risk-based enforcement allowing the STA to effectively use its limited resources to optimize revenue mobilization for the Republic of Serbia

TAMP is conceived as an institutional reform project focusing on core tax administration functions and comprising four components: (1) Legal Environment; (2) STA Organization and Operations; (3) ICT Systems and Records Management Modernization; and (4) Project Management and Change Management. In addition, TAMP will finance technical assistance, training and capacity building, and investments in IT systems and data management.

Component 3: ICT System and Records Management Modernization: The component will improve and expand the services provided by the ICT system and address the STA's serious records management issues, including dealing with the significant paper records backlog.

Information Systems: This sub-component will acquire an "off-the-shelf" tax administration software package that will be used to redesign field operations and the required legal framework to meet its processing requirements. In addition, this sub-component includes an evaluation of the need for an upgrade of the STA's ICT infrastructure.

Although there is a structured institutional risk assessment process, there are no ICT-specific business continuity exercises or impact analyses. The Tax Administration manages its operational risks in a structured manner using a formal risk assessment methodology, a business impact analysis using the World Bank template was conducted for the period 2018-2020, and a well-defined business continuity plan was developed. The business continuity plan included recovery time and recovery point objectives that were established and documented, and strategies were also defined to address these issues. Exercises related to business continuity, such as fire drills, are conducted every three years, and the results are documented. However, there are no special ICT exercises regarding business continuity or business impact analysis activities. The STA management has not yet formally adopted the updated Business Continuity Management Plan for 2021-2023, including the COVID pandemic's risks and related response.

The STA does not test, monitor, or evaluate the effectiveness of the business continuity plan. Neither the internal audit department nor external auditors tested or controlled the point of the business continuity plan.

Objective

The purpose of the assignment is to provide Information Security penetration testing and an operational framework review assessment. In addition, the Consultant shall review the STA security operational framework and conduct external and internal penetration tests.

Scope of Works

The scope of assignment for consulting services should be broken into four phases:

1) **Initial security audit,** which must include:
   - security audit of the whole ICT environment, including cybersecurity risk and compliance (compliance monitoring, issue, and corrective action planning),
   - security program (security strategy of STA IT systems, drafting of IT security act, as well as other internal acts which arise as an obligation prescribed by the legislation of the Republic of Serbia, governance, exception management),
   - governance model (for ICT, cyber security) and Enterprise Architecture,
   - third-party management (evaluation and selection, ongoing monitoring),
   - identity and access management (account provisioning, privileged user management),
   - threat and vulnerability management (threat modeling and intelligence, penetration testing),
   - data management and protection (data classification and inventory, breach notification management),
   - risk analysis (information gathering and analysis),
   - crisis management and resiliency (recovery strategy, policy, and procedures, recovery testing),
   - security operations (change control, configuration management, security architecture),
   - security awareness and training (security training, security awareness, third-party responsibilities).

2) **Penetration Testing Phase**
   - External penetration testing will be tested from an unauthorized perspective and performed completely external to STA via the Internet with no specific network information provided to the vendor. The scope of this review is all Internet-accessible systems owned and operated by STA. The Consultant must perform initial searches and scans to identify targets and potential vulnerabilities. Once vulnerabilities are identified, the Consultant shall validate the potential vulnerabilities and assess the risk associated with each.
   - Internal penetration assessment will be performed inside the organization, mimicking an attacker with internal network access and no credentials. The approach will be the same as in the external penetration assessment.
   - The wireless penetration assessment phase will be performed onsite at the STA Head Quarters and offices in Belgrade. The goal will be to identify wireless networks and validate security mechanisms to prevent unauthorized access through wireless networks.

3) Based on the initial security audit**,** an **Operational framework review** must include:
   - Preparation of risk mitigation plan with included technical, organizational, and administrative measures, aligned with priorities and definition of the timeline of its implementation,

- Definition of security configuration and operations standards for security systems and applications,
- The proposition of cyber security strategy implementation aligned with ongoing projects, business plans, ICT governance model, and Enterprise Architecture of the STA.
- Assessment of current situation regarding Enterprise architecture

4) Based on the adopted risk mitigation plan by STA**, the Monitoring phase** will include:
- Implementation of measures, while the STA will be responsible for the level of implemented measures;
- The Consultant shall monitor implementation with periodic security audit tests every four (4) months until the end of the assignment.

Service delivery

During the assignment, the STA requires written documentation of the approach, findings, and recommendations, as well as assistance in drafting all internal acts of the STA that relate to ICT security and arise from the obligations prescribed by the Republic of Serbia. In addition, a formal presentation of the findings and recommendations to the STA management will also be required.

The documentation should consist of the following:

- EXECUTIVE SUMMARY REPORT: A document developed to summarize the scope, approach, findings, and recommendations in a manner suitable for senior management and the IT team
- DETAILED TECHNICAL REPORT: A document developed for the use of STA technical staff which discusses: the methodology employed, positive security aspects identified, detailed technical vulnerability findings, an assignment of a risk rating for each vulnerability, supporting detailed exhibits for vulnerabilities when appropriate, and detailed technical remediation steps
- RISK MITIGATION PLAN: A document developed for the use of STA with included technical, organizational, and administrative measures that should be implemented

Term and Location of Services

The services associated with implementing these requirements and the accompanying Contract shall be carried out in Belgrade, the Republic of Serbia. Therefore, in addition to attending the STA Headquarters, one may be required to visit offices and sub-offices in Belgrade and some of the surrounding area.

Duration

The duration of this assignment is 18 months from the signing of the Contract, while it is expected that at least 60 man-days should be performed onsite, in direct communication with the STA IT department officials.

Qualifications

Qualification criteria

The prospective Consultant(s) for this assignment is expected to meet the following minimum qualification requirements:

Company

a) The Consultant must be a legal entity;
b) The Consultant must have proven experience and track record in the field relevant to the scope of the service in the last seven (7) years respectively (2015-2021) – a minimum of three (3) projects in ICT security audit, including cyber security risk and compliance or ICT security policies.

As proof, the Consultant shall prepare a table listing the following information: name of the relevant assignments, the short scope of work, year of Contract's implementation, country/region, and Contact reference (name, e-mail, phone number).

Personnel

1) ***Team Leader / Cyber Security Expert***. At least one of the proposed staff (CV must be enclosed) must have:
    a. University Degree;
    b. Minimum of 10 years of professional experience in the implementation of network security and cyber services in large enterprises or public institutions;
    c. Proven experience of at least three (3) similar engagements at public or private institutions;
    d. Certificate in cyber security;
    e. Certificate in Enterprise architecture;
    f. Certificate in the Control objectives for information technology;
    g. Security Certificate issued by Office of the National Security and Intelligence Council (nsa.gov.rs)
    h. Fluency in Serbian is a distinctive advantage;
    i. Experience in managing such assignments and staff;
    j. Excellent communication skills, both written and verbal;
    k. Ability to work in a team.

2) ***Information Security Expert.*** At least one of the proposed staff (CV must be enclosed) must have:
    a. University Degree;
    b. Minimum of 10 years of professional experience in implementation of ICT information standards/solutions in large enterprises or public institutions;
    c. Proven experience of at least three (3) similar engagements at large public or private institutions regarding data privacy;
    d. Certificate in Information Security (ISO27001 or equivalent);
    e. Security Certificate issued by Office of the National Security and Intelligence Council (nsa.gov.rs)
    f. Certificate for Personal Data Protection (certification scheme compliant with the international requirements of the UNI CEI EN ISO / IEC 17024 standard) should be taken as an advantage;
    g. Fluency in Serbian is a distinctive advantage;
    h. Excellent communication skills, both written and verbal.

For both experts, the following **Evaluation criteria** will be applied:

i. Previous experience with World Bank or EU projects will be an advantage
ii. Previous experience with Tax Administration assignments will be an advantage

Evaluation

The Consultant will be selected in accordance with Consultant's Qualifications Based Selection (CQS) as set out in the ***World Bank's Procurement Regulations for IPF Borrowers – Procurement in Investment Project Financing Goods, World, Non-Consulting and Consulting Services, July 2016, revised November 2017 and August 2018*** ("the Regulations").

Expressions of interest will be evaluated by applying the following criteria with allocated points:

(i) General experience – 10 points

(ii) Specific experience related to the assignment – 40 points

(iii) Qualifications of key experts – 50

Key experts will be evaluated based on the following criteria and point allocation:

(a) General Qualifications – 20%
(b) Adequacy for the assignment – 60%
(c) Experience in the region – 20%

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

If awarded a Contract, the successful Consultant will be obliged to provide a valid Security Certificate for access to "Confidential" classified documents and data issued by the Office of the National Security and Intelligence Council (www.nsa.gov.rs)

Terms of Payment

The Contract will be the Standard World Bank Lump-Sum Contract for Small Assignments. The payments for services will be based on the deliverables/reports approved by the Project Coordinator. The Contract costs will include remuneration and reimbursable expenses referring to the assignment.

Conflict of Interest

The engaged Consultant must not be involved in any other related activity to this Project.