MINISTRY OF FINANCE AND THE PUBLIC SERVICE

TERMS OF REFERENCE

CONSULTANCY SERVICE
FOR: IT SECURITY TRAINING

January 2020

Institutional Strengthening Programme

STRATEGIC PUBLIC-SECTOR TRANSFORMATION PROJECT

IBRD LOAN NO.: 8406-JM

DEFINITION OF ACRONYMS

ACRONYM	DEFINITION
BizDevOps	Business, Development and Operations. (A shift to highly collaborative cultures with strong focus on teams and collaboration)
eGovJa	eGov Jamaica Limited
GOJ	Government of Jamaica
G2B	Government-to-Business
G2C	Government-to-Citizens
G2G	Government-to-Government
IBRD	International Bank for Reconstruction and Development
ICT	Information Communications Technology
MDA	Ministries, Departments and Agencies
MSET	Ministry of Science, Energy and Technology (formerly MSTEM)
PDO	Project Development Objective
PFMS	Public Financial Management Systems
SPSTP	Strategic Public Sector Transformation Project

1. BACKGROUND

eGovJa is a full service provider of ICT services such as ICT Consultancy, GOJ Validation Web Services, Data Centre (Hosting and Data Storage), Infrastructure Design and Development Services, and Software Development/Acquisition.

With a mandate to provide ICT services to the entire public sector of the GOJ, eGovJa was restructured to support critical business processes of government entities and to enhance the revenue collection capabilities of the Government of Jamaica. The mandate is further expanded in the Vision 2030 ICT Sector Plan that has the following action items assigned to eGovJa:

- Implement a Brand Jamaica portal organized in product streams. This should be done in collaboration with the Jamaica Trade and Invest.
- Assess, re-engineer and automate key government business processes to improve facilitation and service delivery. This should be done in collaboration with the Cabinet Office and the relevant MDAs.
- Develop more efficient electronic systems for engagement in G2G, G2B and G2C transactions. This should be done in collaboration with our parent ministry, MSET.

The range and scope of the services provided by eGovJa have changed dramatically and the organization is now required to service a larger client base, however there has not been a commensurate increase in human and physical resources.

eGovJa is highly dependent on its information technology systems for the effective delivery of Information and Communication Technology (ICT) services to the Ministries, Departments and Agencies (MDAs) of the Government of Jamaica. Constantly changing security threats demands that eGovJa place an increased focus on security and the implementation of appropriate measures to safeguard the information it stores and processes on behalf of its clients.

eGovJa must design and implement a comprehensive set of information security control preserve the confidentiality, integrity, and availability of information against potential threats

and risk exposures that could have adverse effects on the company's objectives and agreed service levels to its clients.

IT Security training is therefore essential to ensuring that staff with IT Security responsibilities develop the skills and knowledge necessary to provide a secure computing environment and ensure that confidentiality, integrity and availability of information is maintained.

Project Funding Overview

The GOJ is the beneficiary of an investment loan from the World Bank. The Strategic Public Sector Transformation Project (IBRD Loan No.-8406-JM) will, inter alia, assist in repositioning of eGov Jamaica Limited to be able to support the Public Financial Management Systems (PFMS).

The Project Development Objective (PDO) of the SPSTP is to strengthen public resource management and support selected public sector institutions in facilitating a more enabling environment for private sector growth. The project has six components. This consultancy falls under Component III: Adaptive Public Sector Approaches to Promote Fiscal Sustainability. The components of the SPSTP are:

- Component I: Strengthening the Public Investment Management System
- Component II: Strengthening the Budget Preparation Process & Results-Based Budgeting
- Component III: Adaptive Public Sector Approaches to Promote Fiscal Sustainability
- Component IV: Modernizing of the Accountant's General's Department.
- Component V: Fostering Industrial Growth and Trade Facilitation
- Component VI: Project Management

Appropriate training for staff with information security responsibilities will assist eGovJa in ensuring that information security related risks are within acceptable limits. By extension, this will also enhance the delivery of ICT services to GOJ and provide medium to long-term support of the Public Financial Management systems under Component 3 of the Strategic Public Sector Transformation Project. This component will support activities that will contribute to the sustainability of GOJ's reform process in public administration, fiscal sustainability and growth.

2. OBJECTIVES

2.1. Security Training

To develop the required competencies in information security, the company must provide staff with the knowledge and skills required to fulfil their security-related responsibilities.

Comprehensive role-based security training will enhance the company's security posture by creating a trained workforce that can adequately protect its systems and applications and provide the capability to respond effectively to security incidents.

The objective of the engagement is to develop and execute a training program that delivers appropriate security training based on the assigned roles and responsibilities of individuals and the specific security requirements of the company. The training will address management, operational, and technical responsibilities.

On completion of the program, all staff with significant security requirements will:

- Understand their role and responsibilities with respect to security;
- Understand how to implement and maintain information security controls;
- Understand how to mitigate risk to information and information systems;
- Monitor the security condition of the systems, applications, or information for which they are responsible;
- Respond appropriately to information security breaches.

2.2. SCOPE

The scope of work is not considered exhaustive and modifications will be considered during the course of the engagement. All changes to the scope of work shall be formally agreed by both parties.

The scope of work includes:

- Developing a program to provide role-based security training to individuals with identified security roles and responsibilities
- Sourcing and delivering specialized security training for staff in the following job functions:
    - Programmers/ Programmer Analysts
    - Systems Administrators
    - Network Engineers
    - Quality Assurance Analysts
    - IT Security Engineers
    - IT Risk Analysts

- Developing and managing the training schedule to minimize impact on day-to-day support responsibilities of participants

The required training includes a combination industry standard certification-based training and product specific training related to security solutions already deployed by eGovJa. Course descriptions are outlined below:

Course	Course Content	Target Group	No. Participants
Computer Forensics	• Computer forensics investigation process • Searching and seizing • Digital evidence collection • O/S specific forensics (windows/Linux) • Acquisition, duplication Recovery techniques • Using forensic tools • Log capture and correlation • Malicious Software Identification • Network traffic analysis • Investigating wireless attacks • Mobile forensics • Reporting	IT Security Engineers, System Administrators	8
Ethical Hacking	• Footprinting and reconnaissance • Scanning networks • Enumeration • System hacking • Malware threats • Sniffing • Social engineering • Denial-of-service • Session hijacking • Hacking webservers & web applications • SQL injection • Hacking wireless networks	Programmers/ Programmer Analysts Quality Assurance Analysts IT Security Engineers	30

	• Hacking mobile platforms • Evading IDS, firewalls, and honeypots • Cloud computing • Cryptography		
ISO27001 Implementation	• Role and structure of an information security policy • How to determine the scope of an ISMS • Developing a management framework • How to structure and manage the ISO 27001 project • How to allocate roles and responsibilities for ISO 27001 implementation • The definition of risk in ISO 27001 • Options for risk assessments • Selecting risk assessment tools • How to carry out an information security risk assessment • The Statement of Applicability (SoA), • Reviewing existing controls and mapping controls to Annex A of ISO 27001 • Communication strategy • Writing policies and producing other critical documentation • The importance of staff and general awareness training • The key elements of management review • How to manage and drive continual improvement	IT Risk Analysts, IT Security Engineers	8

	under ISO 27001 • How to prepare for an ISO 27001 certification audit		
Penetration Testing	• Need for security analysis • TCP/IP packet analysis penetration testing methodologies • Customers and legal agreements rules of engagement • Penetration testing planning and scheduling • Pre-penetration testing steps • Information gathering • Vulnerability analysis • External penetration testing • Internal network penetration testing • Firewall penetration testing • Ids penetration testing • Password cracking penetration testing • Social engineering penetration testing • Web application penetration testing • SQL penetration testing penetration testing reports and post testing actions	IT Security Engineers System administrators Network Engineers Programmers/ Programmer Analysts Quality Assurance Analysts	15
Security Incident Response	• Risk assessment • Incident response and handling steps • Security incident response teams • Handling network security incidents • Handling malicious code incidents • Handling insider threats • Forensic analysis and	IT Security Engineers	4

	incident response • Incident reporting • Incident recovery • Security policies and laws • Handling email and malicious code attacks • Working with law enforcement		
Security Risk Management	• Risk management vocabulary • Benefits of risk management to an organization • Risk management standard (ISO 31000) • Risk management principles • Understanding the risk management framework at a high level • Risk management processes • Risk identification, risk analysis, risk evaluation and risk treatment • Risk assessment tools • Communication and consultation • Monitoring and review	IT Risk Analysts	4
SIEM Administration	As per IBM Security QRadar SIEM Administration and Configuration	IT Security Engineers	6

3. METHODOLOGY

The Consulting Firm is expected to use accepted and proven methodologies for carrying out the assignment. The Consulting Firm should prepare a detailed methodology and work plan indicating how the objectives of the assignment will be achieved.

The work plan submitted should be aided by a Work Breakdown Schedule showing the allocation of time to each of the key components of the project. Detailed scheduling should be provided to support the methodology outlined.

3.1. Training Delivery

Training will be delivered using one of following formats:

- Local on-site instructor-led classroom training
- Online virtual classroom, instructor led

4. COORDINATION/REPORTING RELATIONSHIP

The Consulting Firm will report to and operate under the supervision of the Senior Director, Programme Management Division or her designate.

The Director or her designate will be supported by the PMO and a Steering Committee, who will co-ordinate the review and approval of the documents prepared by the Consulting Firm.

The Steering Committee will have responsibility for the review and approve key deliverables as listed in section 6.

5. DELIVERABLES

The deliverables under this project are as specified in the tables below. All documents submitted should conform to the following minimum standards:

1. Be comprehensive, properly formatted and well presented;
2. Provide justifications for all assumptions;

5.1. INFORMATION SECURITY TRAINING

The key deliverables for the information security training are as specified in the table below.

The Consulting Firm should bring real-world experience to every workshop. Participants should be led through a combination of presentations and practical hands-on exercises.

The proposal must include a training plan as outlined in the table below.

Key Deliverables	Performance Standard
Training Plan	For each course included the scope of work: - A detailed course outline satisfying the course objectives stated in Scope of Work. - The number of teaching hours (not including breaks) and session options - Optimal class size - The entrance and exit competencies - The training approach and methodology which will be used - The student evaluation methodology - Student material which will be provided, including the medium and rights and restrictions for the use of the training material - Must indicate whether certification exam is included - Details of instructor's experience and certification A training schedule including the following; course, course date(s), duration, class size Any other specific requirements for successful delivery in accordance with this training
Training Delivery	Must include: - Learning objectives for each course - Duration of each course - Manual/documentation - printed (and electronic where applicable) copies of the training material – one for each participant and one for the eGovJa Information Resource Centre - Teaching aids - Delivery of courses on the agreed dates for the identified target audience - Provision of course participation certificates
Training Evaluation Report	This report should contain but not be limited to: - A brief overview of the training with an emphasis on the most important points - Background information on the training program, the objectives and the questions it seeks to answer - Overview of evaluation results and key issues identified

At the end of each course, participants will be asked to complete eGovJa's training evaluation forms.

5.2. "Sign-off" Procedure

The Steering Committee will work with the Consulting Firm to ensure the deliverables align with the objective of this assignment. It is also expected that the Consulting Firm will present the deliverables to the Steering Committee.

5.3. Variations

All proposed changes to the work plan and deliverables must be discussed with the Project Sponsor, and where necessary will be submitted for approval to the Steering Committee.

5.4. Schedule of Payment

Payments for the services will be specified in the Contract.

6. QUALIFICATION AND TECHNICAL EXPERTISE REQUIRED

6.1. The Consulting Firm

The Consulting Firm should have the following minimum qualifications and demonstrated competencies:

a) At least five (5) years' experience working with large organizations to deliver IT security training of a similar scope.

b) Demonstrated evidence of the validity of experience and qualification, including work done for an IT organization.

c) Accredited to deliver training at the requisite level.

d) Must have established partnership arrangements with relevant training & certification bodies.

6.2. Key Skills/ Qualifications

The firm must demonstrate that they have key personnel with skills and/or qualification deliver training in the areas outlined below.

6.2.1. Information Security Training

a) Individual instructors must be certified to teach the respective courses.

b) Individual instructors must be practitioners in the relevant domain with at least 5 years' experience and demonstrated competence.

c) Must be fluent in English.

7. CHARACTERISTICS OF THE CONSULTANCY

Type of consultancy:	Consulting Firm
Duration of Contract	Executed over 12 months
Place of Work:	Jamaica, at eGovJa Offices
Type of Contract:	Fixed Price Contract
Payment Responsibility	MOFPS Project Office
NB: The contract amount includes all costs related to undertaking the consultancy.	

APPENDIX 1: Short listing Criteria

1. The Consulting Firm's experience in delivering training of similar scope as defined by the terms of reference (as per section 6.1 a).

APPENDIX 2: Evaluation Criteria for Scoring TECHNICAL PROPOSALS

	Evaluation Criteria	Maximum Points
	1. Adequacy of qualification and experience of the Consulting Firm for the assignment	***30***
	1.1. The Consulting Firm has a minimum of five (5) years' experience in delivering training of similar scope as defined by the terms of reference.	*10*
	1.2. The Consulting Firm has established partnerships with the relevant product vendors and certification organizations.	*10*
	1.3. The quality of the references provided by previous clients.	*10*
	2. Adequacy and quality of the proposed training plan in responding to the Terms of Reference (TOR): Training Plan reflects a clear understanding of the assignment and suitably responds to each element of the scope of work and deliverables	***40***
	3. Adequacy of Qualification and Experience of the Instructors	***30***
	3.1. Instructors are accredited to teach respective course (mandatory)	
	3.2. Experience in successfully delivering respective training in the past five years: • Four or more courses, four in the last 5 years (15); or • Four or more courses, three in the last 5 years (10); or • Three courses, at least two in last 5 years (6).	15
	3.3. Practical experience in the relevant domain • Five years or more (15 pts); or • Three to Four years (10 pts); • Two years (6 pts)	15
	3.4. Fluency in English (mandatory)	
	Total	***100***

The Consulting Firm is required to meet the minimum score of 70% in relation to the criteria listed in the table above.

The Degree of Responsiveness to the Requirements

1. The procuring entity will assess the Consulting Firm's response to each requirement as follows:

Degree of Responsiveness	***Score***
Excellent	*95 - 100%*
Very Good	*80 - 94%*
Good	*70 - 79%*
Satisfactory	*60 - 69%*
Poor	*50 - 59%*
Unsatisfactory	*0 - 49%*

2. The degree of responsiveness will be used to determine what percentage of the maximum scores allocated for each requirement is attained by each bidder.