Draft

Leveraging ICT for Growth, Employment and Governance Project
Bangladesh Computer Council (BCC)
Information and Communication Technology Division
Ministry of Posts, Telecommunications and Information Technology
ICT Tower, Plot # E-14/X, Agargaon, Dhaka-1207,
Bangladesh

Terms of Reference

For

Information Security Specialist
(Contract Package # S31A-S31D)
(Credit # 5911-BD)

January 2018

Terms of Reference (TOR)
For
Information Security Specialist
(Contract Package # S31C-S31D)

1. Background

Bangladesh Computer Council (BCC), an organization of Information & Communication Technology Division, Ministry of Posts, Telecommunications and Information Technology has received financing from the World Bank toward the cost of the Leveraging ICT for Growth, Employment and Governance (LICT) Project (IDA credit no.: 5911-BD) and intends to apply part of the proceeds for payment of services related to Consultancy for Information Security Specialists.

The project consists of three components: (i) IT/ITES Industry Development, (ii) E-Government and (iii) Project Management Support.

The project development objectives are to: (i) Catalyze the growth of Bangladesh’s IT/ITES industry for employment creation and export diversification; and (ii) Strengthen IT/ITES facilities, policies, standard and guidelines for public sector modernization.

2. Objective of the Assignment

The objective is to recruit a person for the position of Information Security Specialist in order to achieve organization goals by defining, integrating, and upgrading comprehensive information system architecture; managing projects and computer security.

3. Scope of Work

3.1 Description

The Information Security Specialist is responsible for understanding and responding to threats to the security of all information, networks, and computer systems, whether on-premise or cloud. The individual taking the role will monitor a variety of services and tools (including the Managed Security Service, the firewalls, third party sensor/detector/rating services, internal account activity tools, and threat information services) in order to predict, detect, and diagnose threat activity, and direct or participate in containment, eradication, and restoration activities in collaboration with other team in the IT organization and the business.

3.2 Responsibilities

Information Security Specialist would be responsible for the following:

- Monitor information systems, computers and networks to detect cyber threats and respond to cyber threats and finally to remediate information security threats and vulnerabilities
- Analyze, design, and facilitate capabilities, solutions, or preventative/remediation controls to protect proprietary/confidential data and systems in accordance with industry standards and governance/compliance requirements
- Synthesize solution design, architectural patterns, policy and regulatory frameworks, privacy considerations, and risks in the creation of holistic solutions that span technologies and capabilities
- Support the front-line defense of networks, protecting information from unauthorized access and violations. Analyze and assess potential security risks, develop plans to deal with such incidents by putting measures in place such as firewall, IPS, SIEM and

encryption, monitoring and auditing systems for abnormal activity, and executing corrective actions. Prepare technical reports.

- Carry out tests on a system to expose weaknesses in security. Essentially, do everything a hacker would do, but do it on behalf of the organization who owns the network. This means will try to access information without usernames and passwords, and will try to break through whatever security applications are in place. Report findings and then suggest what upgrades/solutions to be implemented.
- Recover deleted files; analyze and interpret data linked to crime; analyzes computer logs and mobile telephone records; and uncover links between events, groups and individuals through pursuit of data trails.
- Work across LINUX, Windows platforms and technologies to design holistic security designs that treat identified risks and enable strategic and/or tactical business or IT solutions
- Research/investigate emerging business application security topics, threats, capabilities, and solution options to create/update policy and governance, technology strategies, solution architecture, and vulnerability assessments
- Applies industry standard risk management technique like ISO/IEC 31010:2009 and knowledge across various business application security capabilities (i.e. technical, application, data and mobile) to determine effectiveness of controls and to create action plans that remediate identified risks
- Participate in and/or lead vendor product reviews, evaluations, demonstrations, proofs of concept and implementations
- Apply broad-based knowledge of security technologies with an in-depth/specialized knowledge of security tools like Nmap, Open VAS, Snort, Wireshark. Kali Linux, etc. to perform daily tasks
- Coordinate security related activities
- Apply systems analysis techniques, including consultations with users to determine security specifications

3.3 Competencies

- **Analysis:** Identify and understand issues, problems and opportunities; compare data from different sources to draw conclusions.
- **Communication:** Clearly convey information and ideas through a variety of media to individuals or groups in a manner that engages the audience and helps them understand and retain the message.
- **Exercising Judgment and Decision Making:** Use effective approaches for choosing a course of action or developing appropriate solutions; recommend or take action that is consistent with available facts, constraints and probable consequences.
- **Technical and Professional Knowledge:** Demonstrate a satisfactory level of technical and professional skill or knowledge in position-related areas; remains current with developments and trends in areas of expertise.
- **Building Effective Relationships:** Develop and use collaborative relationships to facilitate the accomplishment of work goals.
- **Client Focus:** Make internal and external clients and their needs a primary focus of actions; develop and sustain productive client relationships
- **Ability to frame an architecture strategy** and gain buy-in from both business and IT executives
- **Demonstrated ability to describe non-functional requirements** and translate into architecture constraints
- Experience with government systems and business processes.

4. Qualifications & Experience

4.1. Educational Qualification:

Bachelor's degree in Computer Science, Information Security, or Information Systems Management

4.2. Work Experience:

- Minimum Eight (8) years of experience working daily with network or host-based threat detection technologies.
- Must be pro-active and a self-starter as this position requires a lot of independent work.
- Knowledge of networking technologies and protocols, including Ethernet, VLANs, TCP/IP and routing.
- Experience with security technologies including: Vulnerability Scanning, Firewalls & Log Analysis, Host-based detection tools, Security Event and Incident Management (SEIM), Antivirus, Network Packet Analyzers, malware analysis and forensics tools.
- Experience in analyzing audit logs, router logs, firewall logs, IDS logs and TCP/IP headers.

4.3. Certification:

At least 2 certifications among the following: CCNA, CCNP, CEH, OSCP, CHFI, Sec+.

5. Reporting Arrangements

The Information Security Specialist will assist and report to the Project Director, under the general supervision and guidance of the e-Government Team Leader and CIRT Team Leader.

6. Duration of the Assignment:

The duration of the assignment will be about 16 months and may extend subject to satisfactory performance of the Consultants & Project Extension.

7. Facilities to be provided by the Client:

Project will provide appropriate office space and other associated (data, information, furniture, stationeries, etc.) necessary to carry out the assignment.

8. Reporting requirements/deliverable:

The Information Security Specialist will need the following reporting requirements/deliverables, but not limited to:

- Monthly work plan and progress report;
- Yearly report
- Any other Report, as required.