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

Risk Analyst
(Contract Package # S33A-33B)
(Credit # 5911-BD)

January 2018

Terms of Reference (TOR)
For
Risk Analyst
(Contract Package # S33A-33B)

1. Objective of the Assignment

The objective is to recruit two (2) Risk Analysts for evaluating risk associated with the use, ownership, operation, and adoption of IT systems of the Government of Bangladesh. The Risk Analyst will support the risk identification and management process across all aspects of Information Technology. Responsibilities include assessing the current adequacy of the security strategy, business continuity /disaster recovery plans, threats to the systems, and then calculating the impact of potential adverse events. Audits and assessments must be continual, as the threat profiles change constantly. The Analyst will keep executive management up to date on the results of the risk assessment and make recommendations for mitigations to protect their systems or cover potential losses.

2. Scope of Services

The Risk Analyst will be responsible for the following:

Identification:

- Identify risks which might occur
- Identify likelihood and impact of risks
- Identify vulnerabilities or weaknesses in systems;
- Identify appropriate controls to effectively manage information risks as needed
- Identify defensive steps to take, including necessary firewalls, security software and data encryption;
- Identifying breaches in organization's security and track the source of an unauthorized intrusion.
- Identify opportunities to improve risk posture

Assessment/Evaluation:

- Perform focused risks assessments of existing or new services and technologies
- Evaluate and Assess the residual risk
- Examine employee compliance with security controls and deficiencies;
- Evaluate security policy, processes and procedures for completeness;
- Continuously evaluate communication security, data vulnerability, business continuity and compliance risks;

Providing Solution:

- Develop solutions for remediating or mitigating risks
- Provide consultative advice to data center customers that enable them to make informed risk management decisions.
- Provide mitigation/ damage reduction proposals with cost justification.
- Recommend all infrastructure and applications patching and remediation be done;

- Stay knowledgeable of current advances in all areas of information technology concerning vulnerabilities, security breaches or malicious attacks;
- Ensure that controls are adequate to protect sensitive information systems;

Documentation/Reporting/Communication:

- Communicate risk assessment findings to information system owners
- Report to management on IT system vulnerability and protection against malware and hackers;
- Clearly document and define risks and potential impacts along with the statistical probability of such an event and identify systems affected by the defined risk;
- Communicate recommended business continuity preparations and controls, including deficiencies, to business units.
- Recommend improvements in network security, identity management and logging
- Maintain strong working relationships with individuals and groups involved in managing information risks across the organization

3. Education and Experience

- Minimum Bachelor's degree in Information Technology/ Computer Science/ Computer Engineering (or similar)
- Minimum Eight (8) years of progressive experience in computing and information security, including experience with Internet technology and security issues required
- Experience should include security policy development, security education, network penetration testing, and application vulnerability assessments, risk analysis and compliance testing
- Working Knowledge of information security standards (e.g., ISO 17799/27001, etc.), rules and regulations related to information security and data confidentiality and desktop, server, application, database, network security principles for risk identification and analysis
- Strong analytical and problem solving skills
- Excellent communication (oral, written, presentation), interpersonal and consultative skills.
- This position requires some weekend and evening assignments as well as availability during off-hours for participation in scheduled and unscheduled activities
- Certified in Risk and Information Systems Control (CRISC) Certification is highly desirable
- Experience in large company and/or financial services organization preferred
- Experience in project/program management for technology and/or risk initiatives preferred
- Other IT governance/policy experience helpful
- IT operational experience helpful
- ITIL and COBiT Certifications helpful

4. Reporting Arrangements

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

5. 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.

6. 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.

7. Reporting requirements/deliverable:

The Risk Analyst will need the following reporting requirements/deliverables, but not limited to:

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