Brief Terms of Reference (TOR)

Requirement Gathering and Risk Assessment of Government Organizations

1. Background

Sri Lanka CERT under the guidance of the Ministry of Technology aims to implement the Information and Cyber Security Policy for Government Organizations. Information and cyber security risk assessment is a critical activity of the implementation of the Policy to determine an organization's ability to protect its information and IT assessment from cyber threats. Therefore, as the first step of the implementation of the Policy, Sri Lanka CERT aims to procure a qualified and experience firm to conduct risk assessment of selected government organizations that maintain critical information infrastructure.

2. Scope Objectives of the Study

a. Conduct a comprehensive process based information security risk assessment on ten (10) government organization maintaining critical information infrastructure
b. Development of Risk Register for the organization
c. Development of Risk Treatment Plan in consultation with government organizations.

3. Specific Activities of the Assignment

a. In consultation with Sri Lanka CERT, develop of IT Risk Assessment Framework based on Information and Cyber Security Policy to assess the Information Security Risk.

b. Based on the developed IT Risk Assessment Framework, perform a General IT Control review, and comprehensive Risk Assessment on the IT operations of the organization.

c. Development of report which includes the ITGC Observation Log,

d. Development of report on IT Risk including Risk Register. All IT risk should be converted to organization's business risks.

e. Development Risk Treatment Plan in consultation with Respective organizations.

4. Government Organization

a. Conduct above activities for the Ten (10) organizations assigned by Sri Lanka CERT.

b. Upon the selection of a qualified and experience firm through competitive bidding, Sri Lanka CERT shall assign Ten (10) organizations for the assignment.

5. Qualification of Key Staff

Consultant is free to propose the number and structure of experts appropriate to his implementation approach, provided that the team properly covers the above-mentioned functions. The suggested staff positions qualification and experience required for this assignment is presented in the table below.

Key Staff	Minimum Academic Qualification	Minimum Experience	Minimum Number of Similar Assignments Conducted
Project Coordinator	Bachelor's Degree from a recognized university. Professional qualifications in Project Management such as PMP/PRINCE 2 will be an added qualification.	Minimum 3 years demonstrated experience in managing research projects	At least 5 similar assignments
Information Security Auditor/Consultant	Degree in Information Technology/Information Security or related field from a recognized university and Professional RISK & information security related qualifications in ISO27001 Lead auditor or CISA . CISSP would be an added qualification.	– Minimum 3 years of demonstrated experience in GRC domain and – minimum 2 years experience in Information Systems Auditing – Demonstrated experience in conducting risk and impact assessments – Demonstrated experience in working with CII projects would be an added experience.	At least 5 IT ISO 27001 Internal Audits or ITGC Audits
IT Risk Advisory Auditor	Bachelor's Degree related to Information Technology/Information Security from a recognized university and Professional qualifications in CISA or ISO 27001 lead auditor. In-depth understanding of ISO 31000 would be an added qualification.	– Minimum 3 years of demonstrated experience in the IT risk advisory, and – Demonstrated experience in conducting risk and impact assessments, and – Demonstrated experience in developing IT risk registers and risk treatment plans	At least 5 Risk assignments Assignments completed in the CII projects would be an added experience

6. Key Deliverables and Payment Schedule

Duration of the assignment is 32 weeks. Consultancy firm shall develop delivery schedule in consultation with Sri Lanka CERT. Deliverables will be reviewed by a committee appointed by the Sri Lanka CERT.

Task	Deliverable	Deadline	Payment as % of Total payment
1. Develop a Risk Assessment Framework	– Development of Inception Report which include, Project Plan, Resource, and Time Schedule and Development Risk Assessments Framework	Contract award date + Week 1	5%
2. Conduct ITGC and Risk Assessment for an organization	– Report which includes the ITGC Report on IT Risk including Register, and Risk Treatment Plan	According the Consultancy Firm's delivery schedule	9% of the Total Payment (10 organizations 90%)
3. Completion Report	– Summary report on all organizations information security status	Contract award date + Week 32	5%