Terms of Reference

Procurement of a Consultancy Firm to Implement Information Security Management System (ISMS)

1. Introduction

Founded in 2006, the Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT) is the National Centre for Cyber Security, which has the national responsibility of protecting the nation's cyberspace from cyber threats. Sri Lanka CERT is currently in the process of implementing standards on Information Security Management System (ISMS) ISO27001:2022.

2. Objectives

Sri Lanka CERT wishes to obtain a qualified and experienced firm to,

- establish, implement, maintain, and continually improve Information Security Management System in alignment with ISO 27001:2022 standards and organizational objectives, and
- The implementation of above standard shall cover the operations of CERT including operations of Digital Forensic Lab and National Cyber Security Operations Centre (NCSOC).

3. Scope of Work

The Consultant is required to conduct the following activities

3.1.Implementation of ISO27001:2022 (Phase I)

3.1.1. ISO 27001:2022 Planning & Gap Analysis

a. Overall project plan for ISO 27001 and 27035 standards implementations
b. ISMS Project Charter and Implementation Roadmap
c. Gap Analysis Report
d. ISMS Scope Document
e. Stakeholder Engagement Plan

3.1.2. Risk Assessments and Management

a. Risk Assessment Report with Risk Register
b. Risk Treatment Plan (RTP)
c. Risk Appetite, Tolerance Level and Acceptance Criteria
d. Statement of Applicability (SoA)
e. Asset Inventory & Classification

3.1.3. ISO 27001:2022 ISMS Framework/Documentation Development

Sri Lanka CERT has developed the policies and procedures covering some of the following areas; hence consultant is required to review the existing documents and identify the gaps, and update and develop necessary documents to fulfill the objectives of the assignment.

a. ISMS Framework Design
b. ISMS Manual
c. Information Security Policy
d. Risk Management Procedure
e. Access Control Procedure
f. Cryptography & Data Protection Procedure
g. Business Continuity & Disaster Recovery Plan
h. Incident Management Procedures
i. Supplier/Vendor Risk Management Procedure
j. Security Awareness & Training Procedure
k. Change Management Procedure
l. Internal Audit Procedure & Checklist
m. Roles & Responsibilities Matrix for ISMS Governance
n. Acceptable Use Policy
o. Patch Management Procedure
p. Password Management Policy
q. Internet and Email Security Procedure
r. Configuration Management Policy
s. Backup and Recovery Management Procedure
t. Cloud Security Policy
u. Remote Working and Mobile Working Procedure
v. Physical and Environment Security Procedure
w. Data Centre Management Procedure
x. Asset Management Procedure
y. Capacity management
z. Network Security Procedure
aa. Threat Intelligence Procedure
bb. PII Protection and Privacy Policy
cc. Malware Management Procedure
dd. Software Licensing Management Procedure
ee. Information Classification Procedure
ff. Removable Media Management Procedure
gg. Logging and Monitoring Procedure
hh. Forms, NDAs and any other related documents required to implement each above Policies and Procedure

3.1.4. ISMS Implementation

a. Implement information security policies and procedures covering above steps
b. Implement technical and administrative controls
c. Conduct training and awareness programs for staff (venue will be provided by CERT)
d. Deploy monitoring and measurement systems
e. Security Control Effectiveness Metrics

3.1.5. Internal Audit & ISO 27001:2022 Certification Preparation

a. Pre Audit/Readiness Review Report
b. Corrective Action Plan (CAP)
c. Management Review Meeting Reports
d. Certification Readiness Support/Report
e. Continuous Improvement Plan

3.1.6. Post-Certification Support

a. Support the closure of post-audit non-conformities
b. Provide ongoing **ISMS maintenance** support
c. Monitor KPIs/KRIs, conduct surveillance audits, and advise on continual improvement

3.2. The Consultant shall identify the requirements of ISO implementation of Sri Lanka CERT in consultation with the committee appointed by Sri Lanka CERT to oversee the implementation of ISO standards.

4. Deliverables and Payment Schedule

The initial phase of ISMS implementation is expected to be completed is 28 weeks, with ongoing support and maintenance activities continuing thereafter in. Payment shall be made upon the acceptance of the documents by the deliverable review committee appointed by Sri Lanka CERT.

#	Activity and Deliverable	Duration (weeks & months)	Payment
Phase I: Implementation of ISO27001:2022		**16 weeks**	**100% of the Total Contract Price**
1	**ISO 27001:2022 ISMS Planning & Gap Analysis** Activities of ISO 27001:2022 Planning & Gap Analysis (Reference Section 3.1.1)	Awarded date + week 2	5% of the contract value

2	**Risk Management** Activities of Risk Management (Reference Section 3.1.2)	Awarded date + weeks 4	10% of the contract value
3	**Framework/Documentation** Activities of Framework/Documentation (Reference Section 3.1.3)	Awarded date + weeks 8	5% of the contract value
4	**ISMS Implementation:** Activities of ISMS Implementation (Reference 3.1.4)	Awarded date + weeks 14	30% of the contract value
5	**Internal Audit & Certification Preparation:** Activities of Internal Audit & ISO 27001:2022 Certification Preparation (Reference Section: 3.1.5)	Awarded date + weeks 15	20% of the contract value
6	**Post-Certification Support:** Activities of Post-Certification (Reference Section 3.1.6)	Awarded date + weeks 16	20% of the contract value
7	Conduct awareness, training session for Sri Lanka CERT staff	Awarded date + weeks 15	10% of the contract value

5. Staff Requirement

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 minimum number of staff qualification and experience required for this assignment is presented in the table below. The proposed staff must remain with the contracted firm until the closure of the engagement. Any exceptions will require prior approval from Sri Lanka CERT.

Key Staff	Minimum Academic Qualification	Minimum Experience	Minimum Number of Similar Assignments Conducted
Project Coordinator [01 Position]	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
ISMS Lead Auditor [02 Positions Minimum]	Degree in Information Technology/Information Security or related field from a recognized university and ISO certification related to ISO27001 Lead auditor. CISA/CISM/CISSP would be an added qualification.	Minimum 5 years of demonstrated experience as an ISO lead auditor Demonstrated experience in conducting ISO 27001 auditing Demonstrated experience in conducting risk assessments	At least 5 similar assignments
ISMS Lead Implementator [02 Positions Minimum]	Bachelor's Degree related to Information Technology/Information Security (or related) from a recognized university and Professional qualifications in ISO 27001 lead auditor. CISA/CISM/CISSP would be an added qualification	Minimum 5 years of demonstrated experience as an ISO Lead Implementer. Demonstrated experience in performing ISO 27001 implementation	At least 5 similar assignments