Terms of Reference

Procurement of a consultant for the development and validation of documents in alignment with applicable standards

1. Introduction

The Sri Lanka CERT is currently in the process of establishing the National Cyber Security Operations Centre (NCSOC) with the aim of strengthening the country's capacity for real-time cybersecurity monitoring, proactive threat intelligence sharing, and effective incident response coordination at the national level. The NCSOC will serve as a central hub for detecting, analyzing, and mitigating cyber threats targeting critical national information infrastructure, government institutions, and other key stakeholders.

In order to ensure that the NCSOC functions in line with internationally recognized standards, frameworks, and best practices, as well as to address the unique cybersecurity requirements of Sri Lanka, it is imperative to develop a comprehensive set of technical standards, policies, and operational guidelines. These standards and policies will define the governance structure, operational workflows, compliance requirements, security controls, and collaboration mechanisms necessary for the effective functioning of the Centre.

This consultancy assignment is therefore designed to engage a highly qualified expert with proven expertise in cybersecurity governance, SOC operations, and international standards alignment. The consultant will be responsible for developing a robust framework of technical standards and policies that will support the NCSOC's operational, technical, legal, and governance dimensions, thereby ensuring that the Centre delivers sustainable, secure, and effective cybersecurity services at the national level.

2. Objectives

The primary objectives of this consultancy are to:

a. **Develop comprehensive technical standards** to guide the system, operation and continuous improvement of the NCSOC, ensuring alignment with international frameworks such as ISO 27001, ISO 27035, and the NIST Cybersecurity Framework.
b. **Formulate policies and governance structures** that define roles, responsibilities, and procedures for cybersecurity monitoring, incident response, threat intelligence sharing, and stakeholder collaboration at the national level.
c. **Establish operational guidelines and best practices** for the effective functioning of the NCSOC, covering areas such as log management, data retention, evidence handling, and secure information sharing.
d. **Ensure national alignment** by tailoring technical standards and policies to address the unique cybersecurity requirements, legal frameworks, and critical national information infrastructure of Sri Lanka.
e. **Support sustainability and resilience** of the NCSOC by providing an implementation roadmap that facilitates capacity building, compliance monitoring, and continuous enhancement of cybersecurity services.

3. Scope of the Consultancy

The Consultant shall be responsible for:

a. Assessing and develop comprehensive international best practices and standards applicable for SOC operations (e.g., ISO 27001, ISO 27035, NIST CSF, MITRE ATT&CK, ENISA guidelines).
b. Developing comprehensive technical standards for:
    - Define standards for SOC architecture, infrastructure, and technologies.
    - Establish procedures for incident detection, analysis, escalation, and response.
    - Propose guidelines for threat intelligence sharing, collaboration, and integration with external partners.
    - Log management, storage, data retention, analysis and digital forensics support.
    - Access management/control, monitoring, auditing and reporting.
c. Drafting policy documents covering:
    - Governance, roles, responsibilities and escalation workflows.
    - Data protection, evidence handling, and compliance policies.
    - Policies for information sharing with national and international stakeholders.
    - Alignment with national cybersecurity laws, Data protection law and privacy requirements
    - Incident response and escalation.
    - Data protection, evidence handling, and compliance requirements.
d. Cyber Security Playbooks
    - Triage and Investigation
    - Incident Response
    - Vulnerability Response
    - Threat Hunting
    - Digital Forensics
e. Operational Guidelines
    - Prepare operational guidelines for day-to-day NCSOC functions, including monitoring, reporting, and response coordination.
    - Prepare guidline for capacity building, training, and awareness programs to support sustainability.
f. Delivering the final set of standards and policies, including an implementation roadmap.

4. Consultant's Qualification and Experience

The Consultant (individual) should possess:

Educatioin Qualifications (Mandatory)	B.Sc degree in IT or related
	Masters Degree in Cyber Security or Information Security or related
Professional Qualifications	Certified Information Systems Security Professional (CISSP)
	Certified Information Security Manager (CISM)
	ISO/IEC 27001:2013 ISMS Lead Auditor

Experience	Minimum 10 years of Experience in the Information Security Sector
	Demonstrated experience in working with ISO 27001 standards and other international standards related to cyber security
	Experience in developing and implementing information security standards
	Familiarity with international standards (ISO 27000 series, NIST, MITRE ATT&CK, etc.)
	Demonstrated experience in working with multiple countries, including Sri Lanka.
	Demonstrated experience in working in Governance, Risk, and Compliance (GRC) assessments
	Proven experience in developing information security policies and procedures, as well as implementing ISMS frameworks.
	Experience in SOC establishment, including the development of SOC process manuals and guidelines.
	Experience in stakeholder engagement, facilitation, and preparation of high-quality technical reports.
	Experience in network and system administration at the infrastructure level.

5. Timeframe and Payment Schedule

- The duration of the assignment is 10 weeks.
- Payment will be made on a milestone basis upon satisfactory delivery and acceptance of outputs:

Deliverable	Description	Timeline	Payment (%)
Inception Report	Detailed methodology, work plan, and timeline, identification of stakeholders and resources required.	Within 2 weeks of contract signing	10%
Draft Technical Standards & Policies	First draft of technical standards (log management, incident response, threat intel, access control, etc.) and policy documents (governance, data protection, information sharing, compliance), Operational Guidelines etc.	Within 8 weeks of contract signing	50%
Final Technical Standards & Policies	Submission of final, revised standards and policies incorporating stakeholder inputs and international best practices.	Within 9 weeks of contract signing	30%

Deliverable	Description	Timeline	Payment (%)
Final Report	Final consolidated report with all deliverables.	Within 10 weeks of contract signing	10%

6. Selection Criteria of Consultant

The selection will be based on the following criteria:

#	Evaluation Criteria	Marks
a.	Relevant qualifications and professional certifications (Refer the Section 4. Consultant's Qualification and Experience)	30
b.	Methodology and approach proposed for undertaking the assignment	40
c.	Experience in similar assignments (Refer the Section 4. Consultant's Qualification and Experience)	30

The consultant shall score more than 80 marks to qualify for the assignment.

7. Proposal Submission

Interested Consultants are invited to submit their proposals, which should include:

- Technical Proposal:
  - Understanding of the assignment.
  - Methodology and approach.
  - Work plan and deliverables.
  - Relevant experience and references.
  - CVs of key experts.
- Financial Proposal:
  - Detailed cost breakdown for the deliverables presented in section 5, inclusive of taxes.

8. Additional Considerations *(recommended)*

- **Confidentiality:** All data, reports, and deliverables shall remain the property of the NCSOC and treated as confidential.
- **Coordination:** The Consultant will coordinate closely with the NCSOC team and other stakeholders.

1. Annex

CURRICULUM VITAE (CV) FORMAT

{Notes shown in brackets { } in italic should not appear on the final document to be submitted}

Position /Title	
Name of Consultant:	*{Insert full name}*
Date of Birth:	*{day/month/year}*
Country of Citizenship/Residence	

Education: *{List college/university or other specialized education, giving names of educational institutions, degree(s)/diploma(s) obtained}*

_____

_____

Certifications: *{List professional institutes, giving names of certification name, dates acquired}*

_____

_____

Employment record relevant to the assignment: *{Starting with present position, list in reverse order. Please provide dates, name of employing organization, titles of positions held, contract amount, types of activities performed and location of the assignment, and contact information of previous clients and employing organization(s) who can be contacted for references. Past employment that is not relevant to the assignment does not need to be included.}*

Period	**Employing organization and your title/position. Contact information for references**	**Country**	**Summary of activities performed relevant to the Assignment**
{e.g., May 2012-present}	*{e.g., Ministry of ....., Advisor/Consultant to...* *For references: Tel...../e-mail.....; Mr....., Director General}*		

{e.g., From Jan 2010 to present}			

Memberships in Professional Associations and Publications:

1. _____
2. _____
3. _____

Language Skills:

Language	Excellent	Good	Basic	None
Sinhala				
English				
Tamil				

Note: Please tick in relevant box

Proposal

The consultant shall submit a proposal for the assignment covering the areas of the Terms of Reference. Price of the

Consultant's contact information: (e-mail ....., phone.....)

Certification:
I, the undersigned, certify that to the best of my knowledge and belief, this CV correctly describes myself, my qualifications, and my experience, and I am available to undertake the assignment in case of an award. I understand that any misstatement or misrepresentation described herein may lead to my disqualification or dismissal by the Client, and/or sanctions by the Bank.

Name of Consultant Signature

Date:
{day/month/year}