Terms of Reference

Procurement of an Individual Consultant Service for Preparation of Documentation of the Cybersecurity Capability Maturity Model (CMM) for NCSOC

1. Introduction

The Sri Lanka CERT has established the National Cyber Security Operations Centre (NCSOC), which is now operational and serves as the central hub for real-time cybersecurity monitoring, threat intelligence sharing and incident response coordination for critical national information infrastructure, government institutions and other key stakeholders.

Under a previous consultancy assignment, the NCSOC has already developed its technical standards, policies, cyber security playbooks, operational guidelines and an implementation roadmap, aligned with ISO/IEC 27001, ISO/IEC 27035, the NIST Cybersecurity Framework and MITRE ATT&CK.

As the next step, the NCSOC intends to measure and improve the maturity of its operations using the SOC Capability Maturity Model (SOC-CMM). SOC-CMM assesses a SOC across five domains – Business, People, Process, Technology and Services. Several documents required as evidence under SOC-CMM are not covered by the existing NCSOC documentation set.

This assignment is therefore designed to engage a qualified individual consultant to prepare only those additional documents needed to close the SOC-CMM documentation gaps, building on the documents the NCSOC already holds. Given the limited budget and timeframe, the assignment focuses on a defined, priority set of documents listed in Section 3.

2. Objectives

The primary objectives of this consultancy are to:

a. **Map existing NCSOC documentation to SOC-CMM** and identify the documentation gaps against the agreed target maturity level.

b. **Prepare the priority SOC-CMM documents** listed in Section 3 that are not covered by the existing NCSOC documentation.

c. **Provide a SOC-CMM evidence mapping matrix** linking every SOC-CMM domain and aspect to the NCSOC document(s) that evidence it.

d. **Provide a maturity improvement roadmap** setting out how the NCSOC will progress from its current to its target SOC-CMM maturity level.

3. Scope of the Consultancy

3.1 Out of scope

The following were delivered under the previous assignment "Restructuring of NCSOC Policies and Procedures" and shall not be re-developed. The Consultant shall reference them as existing evidence in the SOC-CMM mapping and recommend minor updates only where necessary.

Area	Existing NCSOC documents
Technical standards	SOC architecture, infrastructure and technologies; incident detection, analysis, escalation and response; threat intelligence sharing and integration; log management, storage, data retention and digital forensics support; access management, monitoring, auditing and reporting
Policies	Governance, roles, responsibilities and escalation workflows; data protection, evidence handling and compliance; information sharing with national and international stakeholders; alignment with national cybersecurity, data protection and privacy laws; incident response and escalation
Cyber security playbooks	Triage and investigation; incident response; vulnerability response; threat hunting; digital forensics
Operational guidelines	Day-to-day monitoring, reporting and response coordination; capacity building, training and awareness
Roadmap	Implementation roadmap for the standards and policies

3.2 In scope

The Consultant must carry out the following tasks:

a. **SOC-CMM gap assessment:** Review the existing NCSOC documents, conduct a SOC-CMM self-assessment with the NCSOC team using the latest SOC-CMM tool, agree the target maturity level with NCSOC management, and confirm the final list of documents to be prepared.

b. **Preparation of documents:** Prepare the priority documents listed in Section 3.3, tailored to the NCSOC as it currently operates.

c. **Evidence mapping:** Prepare a SOC-CMM evidence mapping matrix covering both the existing documents and the new documents.

d. **Validation:** Conduct one validation meeting with NCSOC staff and incorporate feedback.

e. **Roadmap and handover:** Prepare a maturity improvement roadmap and conduct one knowledge transfer session so the NCSOC team can maintain the documents and repeat the assessment.

3.3 Documents to be prepared

The following documents are not covered by the existing NCSOC documentation and shall be prepared under this assignment:

#	SOC-CMM domain	Document	Key content
1	Business	NCSOC Charter	Mission, vision, mandate, constituency, scope of services, authority and review cycle
2	Business	Stakeholder and Constituency Register with SLA Template	Constituents and partners, their requirements and contacts; standard service level agreement template

#	SOC-CMM domain	Document	Key content
3	People	Role Descriptions and Competency Matrix	Job descriptions for each NCSOC role (Tier 1–3 analysts, incident handler, threat hunter, forensic analyst, SOC manager) with required skills and certifications
4	Process	SOC Management and Continuous Improvement Procedure	Planning, periodic review, lessons learned, document control and annual SOC-CMM self-assessment
5	Process	Use Case Management Framework	Lifecycle for detection use cases: request, design, testing, deployment, tuning and retirement, mapped to MITRE ATT&CK
6	Process	Metrics and KPI Framework	Operational and service KPIs (e.g. MTTD, MTTR, SLA compliance), definitions, data sources and reporting frequency
7	Process	Knowledge Management Procedure	Knowledge base structure, case documentation, shift knowledge sharing and staff onboarding
8	Technology	Technology Management Procedure	Asset inventory, configuration and change management, maintenance and capacity management for SOC tools
9	Services	NCSOC Service Catalogue	Description of each NCSOC service with scope, inputs, outputs, service levels and linked playbooks
10	All	SOC-CMM Evidence Mapping Matrix (Excel)	Mapping of each SOC-CMM aspect to existing and new NCSOC documents, with current and target scores
11	All	Maturity Improvement Roadmap	Prioritised actions to move from current to target maturity, with responsibilities and timelines

If the gap assessment shows that an item above is already adequately covered by an existing document, the NCSOC may replace it with another identified gap of similar effort, within the same budget and timeframe.

4. Deliverables

All deliverables shall be in English and submitted in editable electronic format (MS Word / MS Excel) and in PDF.

#	Deliverable	Content
D1	Inception and Gap Assessment Report	Methodology and work plan, SOC-CMM baseline assessment, agreed target maturity level and confirmed document list.
D2	Draft Business, People and Services Documents	Draft documents 1, 2, 3 and 9 in Section 3.3.
D3	Draft Process and Technology Documents	Draft documents 4 to 8 in Section 3.3 and the draft evidence mapping matrix.
D4	Final Documentation Set	All documents in Section 3.3 revised after the validation, and the final evidence mapping matrix.
D5	Final Report	Maturity improvement roadmap, consolidated final report and knowledge transfer materials.

5. Consultant's Qualifications and Experience

The Consultant (individual) should possess the following:

Category	Requirement
Educational Qualifications (Mandatory)	Bachelor's degree in IT, Computer Science, or a related field. and Master's degree in Cybersecurity, Information Security, or a related field.
Professional Qualifications	Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM), and ISO/IEC 27001 ISMS Lead Auditor or Lead Implementer SOC-CMM assessor training or a SOC/incident response certification (e.g. GCIH, GCIA, CySA+) will be an advantage
Experience	• Minimum 5 years of experience in the information security sector and • Demonstrated experience conducting SOC maturity assessments using SOC-CMM or an equivalent maturity framework or • Experience in SOC operations or SOC establishment, including development of SOC process documentation and service catalogues or related services and • Proven experience developing information security policies and procedures with Familiarity with international standards (ISO/IEC 27001, ISO/IEC 27035, NIST CSF, MITRE ATT&CK, etc.) • Demonstrated experience working with government or national-level organisations

6. Timeframe and Payment Schedule

- The duration of the assignment is a maximum of five (5) weeks from the date of contract signing.
- Payment will be made on a milestone basis upon satisfactory delivery and acceptance of outputs:

Deliverable	Timeline	Payment (%)
D1 – Inception and Gap Assessment Report	Within 1 week of contract signing	15%
D2 – Draft Business, People and Services Documents	Within 2 weeks of contract signing	20%
D3 – Draft Process and Technology Documents	Within 3 weeks of contract signing	25%
D4 – Final Documentation Set	Within 4 weeks of contract signing	25%
D5 – Final Report	Within 5 weeks of contract signing	15%

7. Selection Criteria of Consultant

The selection will be based on the following criteria:

#	Evaluation Criteria	Marks
a.	Relevant qualifications and professional certifications (refer Section 5)	30
b.	Methodology and approach proposed for undertaking the assignment	40
c.	Experience in similar assignments, including SOC maturity assessments (refer Section 5)	30
	Total	**100**

The Consultant must score more than 80 marks to qualify for the assignment.

8. Proposal Submission

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

Technical Proposal

- Understanding of the assignment.
- Methodology and approach, including how the SOC-CMM gap assessment will be conducted.
- Work plan and deliverables.
- Relevant experience and references, including at least one SOC maturity assessment or SOC documentation assignment.
- CV in the format given in the Annex, with copies of degree and certification documents.

Financial Proposal

- Detailed cost breakdown for the deliverables presented in Section 6, inclusive of all applicable taxes.

9. Additional Considerations

- **Use of existing documents:** The Consultant shall build on the existing NCSOC standards, policies, playbooks and guidelines, and shall not duplicate their content.
- **Confidentiality:** All data, reports and deliverables shall remain the property of the Sri Lanak CERT/NCSOC and be treated as confidential. The Consultant shall sign a non-disclosure agreement before accessing NCSOC information.
- **Intellectual property:** The NCSOC shall hold full rights to use, modify and distribute all documentation produced under this assignment.
- **Inputs from NCSOC:** The NCSOC will provide the existing documentation, access to relevant staff and facilities for the workshop and knowledge transfer session.
- **Conflict of interest:** The Consultant shall disclose any interest in vendors of SOC technologies or services that may be affected by this assignment.

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 specialised education, giving names of educational institutions and degree(s)/diploma(s) obtained}
Certifications	{List certification names, issuing bodies and dates acquired}

Employment record relevant to the assignment

{Starting with present position, list in reverse order. Please provide dates, name of employing organisation, titles of positions held, contract amount, types of activities performed, location of the assignment, and contact information of previous clients and employing organisation(s) who can be contacted for references.}

Period	Employing organisation and title/position; contact information for references	Country	Summary of activities performed relevant to the assignment
{e.g. May 2018 – present}	{e.g. Ministry of …, Advisor/Consultant. For references: Tel … / email …; Mr …, Director General}		

SOC maturity assessments and SOC documentation assignments completed

Period	Client	SOC-CMM or framework used	Scope and outcome

Memberships in Professional Associations and Publications

1. _____

2. _____

3. _____

Language Skills *(please tick in relevant box)*

Language	Excellent	Good	Basic	None
Sinhala				
English				
Tamil				

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.

Name of Consultant:	Signature:
	Date: {day/month/year}