Terms of Reference (TOR)
SOC 2 Type II Certification for National Cyber Security Operations Center (NCSOC)

1. Introduction

The National Cyber Security Operations Center (NCSOC), operating under the purview of Sri Lanka CERT, plays a critical role in monitoring, detecting, and responding to cyber threats at a national level. Given the sensitive nature of the data handled and the critical infrastructure protected, establishing robust security and operational controls is paramount.

To demonstrate our commitment to the highest standards of security, availability, and confidentiality, the NCSOC is initiating a project to achieve System and Organization Controls (SOC) 2 Type II compliance. This ToR outlines the requirements for a qualified consultancy or certified auditing firm to conduct the SOC 2 Type II assessment and provide the final certification report.

2. Objectives

Objective 1: SOC 2 Readiness & Remediation (Consulting)

1. Assess the NCSOC's current security posture, policies, and procedures against the applicable AICPA Trust Services Criteria (TSC) relevant to SOC 2 Type II.
2. Identify and document any control gaps, providing actionable remediation strategies and implementation guidance to prepare for a formal audit.
3. Guide and train the NCSOC team on SOC 2 Type II requirements to ensure the successful design, implementation, and ongoing maintenance of the control environment.

Objective 2: Formal SOC 2 Examination (Independent Audit)

1. Conduct a formal, independent SOC 2 Type II examination in accordance with AICPA attestation standards (SSAE 18).
2. Provide the official SOC 2 auditor's report, including the independent service auditor's opinion regarding the design and operating effectiveness of the NCSOC's controls.

3. Scope of Work and Audit Methodology

The firm will be responsible for executing the following five-phase methodology:

Phase 1: Scoping and Gap Analysis

1. **System Definition:** Define the system boundaries, infrastructure, data flows, and personnel within the scope of the NCSOC.

2. **Criteria Selection:** Cover all the Trust Services Criteria. (Security is mandatory; Availability, Processing Integrity, Confidentiality, and Privacy will be evaluated for inclusion based on NCSOC's operational requirements).
3. **Gap Assessment:** Conduct a comprehensive gap assessment against all criteria and deliver a detailed remediation roadmap to achieve compliance.

Phase 2: Remediation Support and Readiness Assessment

1. **Advisory Support:** Provide ongoing guidance to the NCSOC team during the implementation of required technical controls, policies, and procedural changes.
2. **Readiness Assessment:** Perform a mock audit to ensure all technical and administrative controls are properly designed, implemented, and operating effectively prior to the formal audit.

Phase 3: Formal SOC 2 Audit Execution

1. **Audit Execution:** Execute the formal SOC 2 Type II audit evaluating control effectiveness over an agreed-upon observation period (6 months).
2. **Policy & Procedure Review:** Thoroughly review all relevant organizational policies, procedures, and established security frameworks.
3. **Control Assessments:** Conduct deep-dive technical and administrative control assessments, including the review of system logs, security configurations, and operational workflows.
4. **Evidence Gathering:** Perform interviews with key stakeholders to gather, review, and validate all necessary audit evidence.

Phase 4: Reporting and Certification

1. **Report Drafting:** Prepare the final SOC 2 Type II report in accordance with international auditing standards. This report will include the auditor's opinion, a detailed system description, and the results of the tested controls.
2. **Management Representation:** Obtain and validate the Management Representation letter.
3. **Certification Issuance:** Issue the final, official SOC 2 report/certificate to the NCSOC.

Phase 5: Post-Certification Recommendations

1. **Continuous Improvement:** Provide post-audit guidelines and strategic recommendations to help NCSOC maintain compliance, continuously monitor controls, and fine-tune its security posture for future audit cycles.

4. Key Deliverables

As part of this engagement, the firm is expected to provide the following tangible deliverables:

1. **Scope and Boundary Definition Document.**
2. **Gap Assessment Report and Remediation Roadmap.**

3. **Readiness Assessment (Mock Audit) Report.**
4. **Final SOC 2 Type II Audit Report issued from Licensed CPA or Audit Firm**. (including the auditor's opinion and system description).
5. **Post-Audit Strategic Recommendation Document** for future compliance maintenance.

5. Qualification Requirements

To be considered for this engagement, the auditing firm and its project team must meet the following criteria for **SOC 2 Type II** attestation:

1. **Firm Credentials & Licensing**

   AICPA Authorization: The firm must be a licensed **CPA (Certified Public Accountant)** firm in good standing and recognized by the **AICPA** to issue formal SOC 2 Type II reports.

   Peer Review: (Recommended) The firm should have a current, "pass" rated peer review report as required by the AICPA to ensure the highest quality of audit standards.

2. **Experience & Domain Expertise**

   SOC 2 Specialization: Proven track record of delivering **Type II** (operating effectiveness) reports.

   Audit History: Must demonstrate at least **three (3) successful SOC 2 Type II Engagements** completed within the last 5 years.

   Technical Environment Expertise: Significant experience auditing Cyber **Security Operations Centers (SOCs)**, managed security service providers (MSSPs), or national-level cyber entities would be an added advantage.

6. Team Qualifications & Certifications

Designation	No.	Key Responsibilities	Domain-Specific Experience	Preferred Qualification
Engagement Manager	1	Overall audit ownership, final review, client approval, audit opinion responsibility Audit planning, control testing oversight, client coordination, report preparation	7+ years in IT audit / assurance	CPA / CISA / CA / ACCA + SOC and ISO27001 Lead Auditor
Senior IT Auditor	1	Conduct control testing, evidence validation, documentation review, Execute audit procedures, collect evidence, perform walkthroughs	3–5 years in IT audit / cybersecurity audit	CISA / ISO 27001 Foundation or equivalent
Information Security Specialist (Technical Reviewer)	2	Validate security controls (EDR, SIEM, IAM, network security), Review cloud security, configurations, access control, logging	4–7 years in cybersecurity operations/security engineering	CEH / Security+ / CISSP / ISO 27001 Implementer + security certifications
Compliance / GRC Analyst	1	Policy review, risk assessment support, compliance mapping	2–5 years in GRC / compliance	ISO 27001 LA / CRISC (preferred) + relevant security certifications

6. **Resumes:** Comprehensive CVs for all proposed staff must be included, highlighting relevant experience and copies of all claimed certifications.

7. Timeframe and Payment Schedule

The total duration of the project is **32 weeks**, depending on the readiness of the NCSOC and the observation period required for a Type II report.

Payments will be made based on the successful completion and acceptance of the following milestones:

Milestone	Phase	Payment %	Estimated Timeline	Deliverable / Trigger
Project Initiation	Phase 1	N/A	Date of Awarded + 2 Weeks	Execution of Contract & Project Kick-off.
Gap Completion	Phase 1	N/A	Date of Awarded + 6 Weeks	Delivery of the **Gap Assessment Report** & Remediation Roadmap.
Readiness Sign-off	Phase 2	40%	Date of Awarded + 12 Weeks	Completion of the **Mock Audit** and confirmation that NCSOC is ready for the observation period.
Audit Commencement	Phase 3	N/A	Date of Awarded + 14 Weeks	Start of the formal observation period and completion of initial Evidence Gathering.
Draft Report	Phase 4	N/A	Date of Awarded + 31 Weeks	Delivery of the **Draft SOC 2 Type II Report** from auditor for management review.
Final Issuance	Phase 4/5	60%	Date of Awarded + 32 Weeks	Issuance of the **Final Signed Report** and Post-Certification Recommendations.

8. Additional Considerations

1. **Confidentiality and Non-Disclosure:** Given the highly sensitive nature of the NCSOC's operations, the selected firm and all assigned personnel will be required to sign a strict Non-Disclosure Agreement (NDA) prior to project commencement.
2. **Knowledge Transfer:** The consultant is expected to conduct workshops and provide active knowledge transfer to the NCSOC internal team to ensure sustainable compliance and internal auditing capabilities post-certification.
3. **Working Language:** All reports, documentation, and communications related to this engagement must be conducted in standard English.
4. **Background Checks:** All auditor personnel requiring physical or logical access to NCSOC facilities and systems may be subject to background verification checks by relevant national authorities.
5. **Data Disposal Certification :** Upon project completion, the firm must provide a formal Certificate of Data Destruction. This document shall certify that all sensitive NCSOC data including system configurations, network diagrams, and screenshots have been permanently and securely purged from the firm’s local devices, cloud environments, and backups in accordance with recognized sanitization standards