Expression of Interest (EOI) Information format for Consulting Firms

1. Project Data & Consulting Firm

Contract Name:	Procurement Of Consultancy Firm to Conduct SOC 2 Certification for the NCSOC
Contract Number:	CERT/GOSL/CON/CQS/2026/05
Name of Consulting Firm:	

2. Eligibility Declaration

We hereby declare that:

(i) We have read the advertisement, and the Terms of Reference (TOR), for this assignment.
(ii) We have not been engaged to prepare such TOR as a firm, sub consultancy, or joint venture; and
(iii) No full-time or part-time or contracted expert employed by our firm, sub consultancy, or joint venture has been engaged to prepare such TOR.

We further confirm that, if any of one or more of our experts is engaged to prepare TOR for any resulting assignment as part of our work product under the assignment to which this advertisement relates, our firm and any such expert(s) will be disqualified from short-listing and/or participation in such follow-on assignment.

Sub-contracting is not allowed for this assignment.

Lead Firm: Name & Address	
Submitting Bids as If JV Provide JV partners details (Copy of the JV agreement should be submitted)	**Single Entity** ☐
JV Partner 1: Name & Address	
Signed by: Position :	

3. Management Competence (Please answer each question in one paragraph of 3-5 sentences)

a. If you are proposing a joint venture (J/V), outline the rationale for and benefits of the "association." Outline proposed management coordination of the "association," including the role of each firm.

b. Does your firm have standard policies, procedures or practices in place that promote quality in: the workplace, your interaction with clients, and the outputs you produce? If yes, describe briefly.

c. How will your firm ensure quality of this assignment?

d. How will your firm deal with any complaints concerning the performance of the staff or the quality of the reports submitted for this consulting assignment? What internal controls are in place to address and resolve complaints?

4. Technical Qualifications including Experience

To be considered for this engagement, the bidding firm (or joint venture) and its proposed project team must meet the following mandatory criteria and provide verifiable evidence for each.

4.1. Firm Credentials, Licensing, and Corporate Profile

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

4.1.2. Peer Review Status: The firm should provide a current, "pass" rated peer review report as required by the AICPA to demonstrate adherence to the highest quality of audit standards.

4.1.3. Business Registration: Provide the firm's history and number of years in business, supported by a valid business registration certificate.

4.1.4. Firm Certifications: The bidder must provide evidence of being certified in ISO 27001 and other relevant internal security standards to demonstrate they practice adequate security themselves.

4.1.5. Corporate Structure: Provide evidence regarding the nature of the firm (Small/Medium/Large, including the total number of employees) and detail the firm's core business and specialized operational areas.

4.2. Firm Experience & Domain Expertise

4.2.1. SOC 2 Specialization: A proven track record of delivering SOC 2 Type II (operating effectiveness) reports. The firm must demonstrate at least three (3) successful SOC 2 Type II engagements completed within the last five (5) years, specifically for high-security environments.

4.2.2. Technical Environment Expertise: Proven experience consulting for or auditing Security Operations Centers (SOCs), Managed Security Service Providers (MSSPs), or national-level cyber entities.

4.2.3. ISO & Framework Experience: Proven experience in the implementation or auditing of ISO 27001:2022, ISO 27035 (Incident Management), and other relevant industry standards (e.g., NIST, GDPR, PCI-DSS).

4.2.4. Risk Management: Proven experience in conducting comprehensive risk assessments and developing risk treatment methodologies.

4.2.5. Referrals: Provide referral details and contact information for clients where SOC 2 implementations/audits were conducted within the past three (3) years.

4.3. Financial and Administrative Capability

4.3.1. Financial Health: The firm must demonstrate financial and administrative strength. Provide detailed figures on Total Revenue, Profit Before Tax, and Profit After Tax for the last three years.

4.3.2. Audited Statements: Provide official, audited financial statements for the last three financial years (e.g., 2023, 2024, and 2025).

4.4. Team Qualifications, Certifications, and Capabilities

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

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

4.5. Value-Added Services

4.5.1. Additional Support Services: Bidders are encouraged to outline any other relevant information or support services they can deliver during this engagement that are not explicitly mentioned in this ToR, which would add value to the NCSOC's compliance posture.