Terms of Reference (TOR)

Selection of Consultancy Firm for preparations for Government Security Operations Center (G-SOC) establishment and Critical Information Infrastructure Protection (CIIP) implementation

Country: Bhutan

Name of Project: Accelerating Transport and Trade Connectivity in Eastern South Asia (Access) – Bhutan Project

Loan No/Credit No/ Grant No: IDA 77560 (Credit)/IDAE4310 (grant)

Assignment Title: Selection of Consultancy Firm for preparations for Government Security Operations Center (G-SOC) establishment and Critical Information Infrastructure Protection (CIIP) implementation

Activity/ Package Reference No: GovTech/CS-3/1

1. BACKGROUND

Bhutan is accelerating its digital transformation as a critical enabler of economic diversification, private sector development, and regional integration. Guided by its 13th Five-Year Plan (2024–2029), the country is prioritizing improvements in digital connectivity to stimulate job creation, attract investment, and modernize trade systems.

To support these national priorities, the World Bank partnered with the Royal Government of Bhutan (RGoB) to develop the "Accelerating Transport and Trade Connectivity in Eastern South Asia" (ACCESS) project. The project was approved by the World Bank Board of Executive Directors in May 2025 and became effective in July 2025.

The ACCESS project includes strategic investments in digital infrastructure and systems that will improve trade efficiency, promote economic activity in underserved regions, and contribute to Bhutan's long-term development goals. The project aims to eliminate manual and paper-based processes and strengthen the resilience of critical systems. These improvements will facilitate seamless regional trade, enhance public service delivery, and bolster Bhutan's capacity to respond to future risks.

To realize the full benefits of these digital investments, Bhutan must also address critical gaps in cybersecurity, as weak digital foundations expose essential services to significant risks. Given ACCESS's emphasis on digital platforms and systems, cybersecurity is integrated as a core element of the project. ACCESS addresses cybersecurity through a dedicated set of activities, including the establishment of a Government Security Operations Center (G-SOC), the development of a Critical Information Infrastructure Protection (CIIP) plan, and the implementation of baseline security measures across key government systems, among others. Together, these initiatives will provide a comprehensive layer of protection for digital trade systems, ensuring their secure implementation and reliable operation.

2. OBJECTIVE OF THE ASSIGNMENT

The objective of this assignment is to conduct preparatory works to guide the establishment of G-SOC, which will be managed by the Bhutan Computer Incident Response Team (BtCIRT), and to develop the CIIP baseline and implementation plan. Specifically, the assignment will strive:

2.1. To develop a comprehensive G-SOC Handbook to guide the establishment of G-SOC.
2.2. To develop a detailed G-SOC establishment workplan to operationalize the G-SOC Handbook.
2.3. To develop a comprehensive CIIP baseline aligned with the CIIP Regulation and the national context.
2.4. To design a phased CIIP baseline implementation plan addressing capacity, technical, and institutional requirements.

3. SCOPE OF SERVICES

The assignment is organized into two main workstreams: (1) the establishment of the G-SOC, and (2) the development of CIIP baseline and implementation plan. While each workstream has a distinct focus, they are inherently interconnected and should be approached in a coordinated and integrated manner. The consultancy firm is expected to propose a clear methodology outlining how the different tasks and activities across these workstreams will be sequenced, aligned, and managed to ensure coherence and efficiency. The detailed scope of each workstream is provided below.

3.1. Inception Report

Before initiating the work on the two workstreams, the consultancy firm will prepare an Inception Report, detailing its proposed methodology, work plan, and team structure. The report will outline how the firm intends to approach and sequence the tasks across the workstreams, ensure coordination and coherence, engage with key stakeholders, and manage risks. It will also include a refined timeline, key milestones, and any initial observations or adjustments based on preliminary consultations or document review. The Inception Report will be presented for review and approval before substantive work begins.

The inception report is expected to be completed and delivered by the end of **Week 4** from the start of the assignment.

3.2. Workstream 1: Establishment of the G-SOC

3.2.1. Deliverable 1: G-SOC Handbook

The main deliverables of Workstream 1 will be a comprehensive G-SOC Handbook, which will serve as the foundational design for the establishment of a Government Security Operations Center (G-SOC) in Bhutan. The conceptualization report will define the strategic, institutional, technical, and operational building blocks required for the G-SOC's establishment and effective functioning. It will articulate the G-SOC’s governance model, institutional alignment, core objectives, functions, collaboration frameworks, technical architecture, and human resource requirements.

The report should be informed by international good practices but tailored to Bhutan’s national context, institutional arrangements, and strategic vision.

The report should include, but not be limited to, the following sections describing the G-SOC:

A. Governance and Institutional Design

B. Participating Institutions and Constituencies.
C. Service Model
D. Operational Framework and Standard Operating Procedures (SOPs)
E. Human Resources and Capacity Requirements
F. Technical Infrastructure and Tools

To develop the G-SOC Handbook, the consultancy firm is expected to perform the following tasks:

3.2.1.1. Desk research and review of Background Materials

Review existing documentation, including, among others, the recently approved National Cybersecurity Strategy (NCS), 13th Five-Year Plan, relevant legal and policy documents, the ACCESS project design documents, and the cybersecurity institutional roles and responsibilities framework.

At the core of the desk research, the consultant should review the G-SOC Comparative Review Note and the G-SOC Institutional Design Note developed under the Advisory Support - Strengthening Cybersecurity Foundations - Phase 3 Technical Assistance, The G-SOC Comparative Review Note provides a benchmarking summary of G-SOC models identified through comparative analysis. The G-SOC Institutional Design Note proposes a preliminary G-SOC model suited to Bhutan's context, defining sections A, B and C presented above; Governance and Institutional Design, Participating Institutions and Constituencies, and Service Model.

This review should serve as the starting point for the consultant's own desk research, ensuring continuity with prior work while allowing expansion into complementary areas – operational frameworks and SOPs, human resources and capacity requirements, and technical infrastructure and tools - and additional aspects the consultant considers relevant for the conceptualization process.

At the end of the desk research, the consultant will synthesize the findings into a Desk Research Summary Note. The note should present key observations from the desk research and outline the consultancy firm's approaches for the G-SOC establishment.

The Desk Research Summary Note is expected to be completed and delivered by the end of **Week 6** from the start of the assignment.

3.2.1.2. Development of initial draft of the G-SOC Handbook

Based on the desk research and the G-SOC Institutional Design Note, the consultancy firm will develop the complementary key sections of the G-SOC Handbook, into an initial draft that will include (but not limited to) the sections described below:

The sections, which were already developed under the G-SOC Institutional Design Note: Governance and Institutional Design, Participating Institutions and Constituencies, and Service Model must be incorporated into the Conceptualization Report as core components. The consultancy firm is expected to integrate these sections into the report, carrying forward the content from the previous note while making any necessary modifications or updates to ensure coherence with the broader conceptualization work:

A. **Governance and Institutional Design:** This section defines the governance structure, strategic objectives, core functions, and guiding operational principles of the G-SOC.

B. **Participating Institutions and Constituencies:** This section identifies all institutions engaged with or served by the G-SOC (e.g., GovTech divisions, regulators, BtCIRT, line ministries, critical sector entities) and outlines their roles and responsibilities, building on the existing cybersecurity institutional framework.

C. **Service Model:** This section defines the suite of services the G-SOC will provide, including their scope, purpose, and delivery mechanisms. The service model should specify the expected service levels for different constituencies, and describe how the services will interact and integrate with one another.

The following complementary sections should be fully developed by the consultancy firm:

D. **Operational Framework and SOPs:** Outline operational processes, workflows, and high-level SOPs. Define collaboration mechanisms such as information-sharing models and escalation paths. Detailed SOPs and operational playbooks will be developed during the implementation phase, based on the specific technical specifications of the GSOC systems to be procured.

E. **Human Resources and Capacity Requirements:** Define the staffing structure and required skill sets for the G-SOC. Recommend training and capacity-building initiatives to support both initial operations and long-term sustainability. Specify clear training objectives and core syllabus components, outlining the core knowledge, skills, and competencies to be acquired. A detailed capacity-building plan will ensure clarity on the training content to be delivered during implementation.

F. **Technical Infrastructure and Tools:** Define the core IT infrastructure and system architecture required for the G-SOC, including hosting models, networking design, and redundancy needs. Identify the cybersecurity tools necessary to enable G-SOC operations (e.g., SIEM, threat intelligence platforms, EDR tools), and provide baseline technical specifications for each category. Review and assess the existing CERT IT infrastructure for potential integration or reuse and recommend any required enhancements or adjustments to ensure alignment and interoperability. These technical specifications will ensure clarity on the requirements to be fulfilled during the implementation.

During the development of the key sections of the G-SOC Handbook, the consultant will prepare a series of short technical notes presenting an initial proposal for BtCIRT review and feedback. These notes will serve as working drafts to support early alignment and facilitate co-creation with BtCIRT on the core design elements of the G-SOC. The technical notes will include:

I. **G-SOC Operational Model Note:** Propose the operational setup, including service offerings drawn from the G-SOC Institutional Design Note, delivery mechanisms, stakeholder engagement, and coordination mechanisms.
II. **G-SOC Capacity Building Requirements Note:** Proposed the capacity building plan, including staffing structure, skill sets, and training needs.
III. **G-SOC Technical Requirements and Tools Note:** Propose the IT architecture, including IT infrastructure, tools, and systems.
IV. **G-SOC Legal Arrangements Note:** Propose the key legal and regulatory provisions required to establish and operate the G-SOC effectively.

These notes will be discussed directly with BtCIRT to further refine and customize the G-SOC plans to Bhutan’s needs and context. Upon BtCIRT approval, the consultancy firm will proceed with consolidating the full report.

The timelines for submitting the technical notes will be decided by BtCIRT and the consultancy firm during the inception report formalization.

It is expected that the consolidation of a full first draft of the G-SOC Handbook will be completed by the end of **Week 18** from the start of the assignment.

3.2.1.3. G-SOC Handbook Validation

Consolidate all findings and proposed frameworks into a draft G-SOC Handbook. Facilitate a two-step validation process. First, conduct a detailed, section-by-section review of the draft report with BtCIRT. This process should be iterative, with each topic presented by the consultancy firm, discussed in depth, and agreed upon. Once this internal validation with BtCIRT is completed, the process should be expanded to include other stakeholders, potentially through targeted in-country workshops or consultation sessions, and incorporate feedback into the final version. The G-SOC Handbook must be developed in close coordination with the development of CIIP baseline. The definition of G-SOC services, constituencies, and operating modalities will be directly influenced by the provisions articulated in the CIIP regulation, particularly regarding the G-SOC’s role in supporting, and monitoring CIIs compliance.

It is expected that the G-SOC Handbook will be finalized by the end of **Week 30** from the start of the assignment. The drafting of the G-SOC Establishment Work Plan (Deliverable 1.2) is expected to begin immediately thereafter and no later than **Week 24** from the start of the assignment.

3.2.2. Deliverable 2: G-SOC Establishment Work Plan

Following the finalization of the G-SOC Handbook, the consultancy firm will develop a comprehensive G-SOC Establishment Work Plan. This deliverable will operationalize the conceptual design into a concrete, time-bound, and costed implementation roadmap, which will serve as a practical guide to establish the G-SOC in a phased and structured manner. It should outline key implementation milestones, required financial and human resources, institutional responsibilities, procurement and capacity-building activities, and risk mitigation strategies.

The work plan must be realistic, actionable, and aligned with the implementation of ACCESS digital components, local capacity, and technical constraints. It should also identify dependencies and sequence activities to ensure smooth rollout. The consultancy firm is expected to collaborate with relevant government stakeholders, technical experts, and the ACCESS PMU to validate and refine the proposed plan.

To develop the G-SOC establishment work plan, the consultancy firm is expected to perform the following tasks:

3.2.2.1. Review of the G-SOC Handbook for Planning Purposes

Revisit the finalized G-SOC Handbook with a focus on translating its content into an actionable implementation plan. Ensure all elements required for planning (governance, staffing, infrastructure, collaboration models) are adequately detailed, and engage stakeholders to confirm assumptions and planning parameters.

3.2.2.2. Development of the G-SOC Implementation Workplan

This task involves developing all core components of a draft implementation workplan, translating the G-SOC conceptual design into a structured and actionable implementation plan. This includes the following elements:

A. **Phasing and Activity Sequencing:** Define the phases of G-SOC establishment (e.g., preparatory phase, pilot phase, full-scale rollout), and break them down into actionable steps and activities. Assign tentative timeframes and define dependencies for each step. The consultant will share the initial workplan outline with BtCIRT for review and feedback by the end of **Week 26** from the start of the assignment, ensuring early alignment.

B. **Resource Planning and Budget Estimation:** Identify required financial, human, and technical resources for each implementation phase. Propose a draft budget and estimate costs across categories.

C. **Procurement:** Define procurement needs and timelines (e.g., hardware, software, services), and recommend procurement approaches and sequencing. A full set of technical requirements and specifications will be prepared separately (see Task 3.2.2.3).

D. **Capacity Building:** Sequence training and knowledge transfer activities identified at the G-SOC Handbook throughout the G-SOC implementation, to meet staffing and operational needs. Identify any additional capacity gaps that could hinder successful implementation. A full skills development plan will be prepared separately (see Task 3.2.2.4).

E. **Institutional Roles and Responsibilities:** Assign roles and responsibilities for implementation oversight, technical delivery, and operational management.

F. **Risk Assessment and Mitigation Planning:** Identify key risks to implementation (e.g., institutional, financial, technical, legal), and propose mitigation measures and contingency plans.

G. **Monitoring and Evaluation (M&E) Framework:** Develop KPIs and milestones to track implementation progress and performance, and propose reporting and review procedures.

It is expected that the first draft of the G-SOC Establishment Work Plan will be submitted for BtCIRT review and feedback by the end of **Week 30** from the start of the assignment.

3.2.2.3. Development of G-SOC Technical Design and Specifications

Develop a comprehensive G-SOC Technical Design and Specifications document that defines all infrastructure, tools, and system requirements necessary for the establishment of the G-SOC. This includes preparing detailed Technical Requirements Specifications (TRS) for all IT components (hardware, software, networking, security tools, and supporting services), as well as minimum technical requirements to ensure performance, scalability, and interoperability.

The TRS will provide an implementation-ready specification package that can be directly used in the procurement process by the implementation vendor.

It is expected that the first draft of the TDS will be submitted for BtCIRT review and feedback by the end of **Week 30** from the start of the assignment.

3.2.2.4. G-SOC Skills Development Plan

Develop a comprehensive skills development plan based on the expertise and roles defined in the G-SOC Handbook. The plan should detail the required competencies, outline clear training objectives, and define the syllabus for each role to ensure the development of the necessary knowledge and skills.

The Skills Development Plan will enable the implementing vendor to propose a tailored program, including specific training courses, delivery methods, and qualified training providers.

It is expected that the first draft of the Skills Development Plan will be submitted for BtCIRT review and feedback by the end of **Week 30** from the start of the assignment.

3.2.2.5. Validation of the Draft Implementation Plan

Present the draft G-SOC Implementation plan, including the Technical Requirements Specifications and the Skills Development Plan, to key stakeholders for feedback and validation, and to ensure alignment with institutional expectations, operational realities and ACCESS timelines and frameworks. This may be done through a dedicated workshop or a series of structured consultations. Feedback will be incorporated into the final version of the work plan.

It is expected that the G-SOC Implementation plan, including the Technical Requirements Specifications and the Skills Development Plan Report will be finalized by the end of **Week 34** from the start of the assignment.

3.2.2.6. Support for Procurement Preparation

Support the preparation of a Terms of Reference (ToR) for the procurement of an implementation vendor, based on the World Bank's procurement process. This includes drafting technical content and other elements of the ToR as requested by BtCIRT for the ToR based on the finalized work plan, outlining deliverables, timelines, required expertise, and technical specifications. Participate in weekly meetings dedicated to the drafting of ToR not exceeding a period of 3 months.

3.2.3. Training and Capacity Building on the G-SOC Handbook

To ensure continuity and institutional memory during implementation, the consultancy firm will arrange a structured capacity-building and knowledge-transfer training for up to 5 (five) officials as nominated by the project. The training objectives shall aim to: (i) Build institutional understanding of the G-SOC as defined in the Handbook; (ii) Enable the trained staff to effectively oversee, supervise, and monitor the subsequent implementation of the system (G-SOC establishment).

The training and capacity-building activities shall be conducted for knowledge transfer and institutional strengthening purposes. The knowledge transfer should be able to help the officials verify the execution of the work plan by the implementing firm. Further, the officials should be able to monitor compliance and provide clarifications or strategic guidance to the implementing firm, ensuring the alignment of the execution of the GSOC elements as per the GSOC work plan. This arrangement will help ensure consistency between the planning and execution phases and enable timely troubleshooting and course correction.

3.3. Workstream 2: Development of CIIP Baseline

The development of the CIIP baseline is expected to translate the CIIP regulation's high level obligations into practical and actionable measures. The baseline will serve as authoritative operational guide for both CII operators and regulators in ensuring consistent implementation and compliance. Beyond technical controls, the CIIP Baseline will also operationalize the principles established in the CIIP regulation by including organizational, managerial, procedural, and physical requirements to provide a comprehensive range of guidance.

This workstream will include two main deliverables:

3.3.1. Deliverable 1: Development of the CIIP Baseline

To develop the CIIP Baseline the consultancy firm is expected to perform the following tasks:

3.3.1.1. Desk Review and Scoping Consultations

Conduct a desk review of the Bhutan CIIP Regulation, relevant policies, strategies, and previously completed work, and examine international good practices in CIIP baselines and related domains. In parallel, hold close consultations with BtCIRT (and, where advised, other relevant stakeholders) to identify the key elements and domains to be included in the CIIP Baseline. This initial scoping will result in an outline of baseline components, which will serve as input for the preparation of the Operationalization Note under Task 3.3.1.2.

It is expected that the outline of baseline components will be presented for BtCIRT approval by the end of **Week 2** from the start of the assignment.

3.3.1.2. Preparation of CIIP Baseline Operationalization Note

Prepare a detailed note setting out the proposed work plan and methodology for translating the high-level requirements of the CIIP Regulation into a practical and actionable CIIP Baseline. The note should outline the sequence of work and roles and responsibilities for each element of the CIIP Baseline. It should also describe the intended scope and objectives, relevant reference materials, expected deliverables, and any dependencies with other elements.

It is expected that the CIIP Baseline Operationalization Note will be finalized and approved by the end of **Week 6** from the start of the assignment.

3.3.1.3. Development of Selected CIIP Baseline Elements

Based on the Operationalization Note and BtCIRT's guidance, develop the specific elements of the CIIP Baseline identified in Task 3.3.1.1. This may include but are not limited to:

- National Cybersecurity Crisis Management Plan
- Asset Management
- Access Control and Identity Management
- Cryptography and Data Protection
- Network Security and Threat Detection
- Cloud Security Baseline
- OT/ICS Security Baseline
- System hardening and configuration/patch management
- Emerging Tech Security
- Third-Party and Supply Chain Security Policy
- Staffing and Cyber Workforce Requirements

For each element, the consultant shall translate international good practices into actionable requirements that are relevant to Bhutan's context. This will require close collaboration with BtCIRT and consultations with other stakeholders, including sectoral regulators and CII operators, to ensure that the requirements are both practical and enforceable. Work on different elements may proceed in parallel, with the consultant organizing and coordinating dedicated mission teams to advance specific elements simultaneously.

Each element under this task shall be presented to BtCIRT and, where relevant, other stakeholders for review and approval before being integrated into the consolidated CIIP Baseline (see Task 3.3.1.4). This ensures that all elements are validated, context-appropriate, and supported by the responsible institutions prior to formal adoption.

3.3.1.4. Consolidation of the CIIP Baseline

Consolidate all developed elements into a single, coherent CIIP Baseline document. Ensure consistency of terminology, structure, and requirements across all domains, and align with the principles established in the regulation.

It is expected that the first draft of the CIIP Baseline document, which includes all developed elements, will be submitted for validation by the end of **Week 24** from the start of the assignment.

3.3.1.5. Validation and Finalization of the CIIP Baseline

Facilitate a validation process for the consolidated CIIP Baseline, potentially through targeted workshops, to present the overall framework that brings together all elements into a coherent and comprehensive product. As stakeholders will already have engaged with the individual stakeholders during their development, the validation will focus on confirming the consistency, completeness, and usability of the full CIIP Baseline.

As part of this task, the consolidated CIIP Baseline shall also be presented to senior leadership of the RGoB to secure high-level endorsement and alignment with national priorities. Feedback from this stage will be incorporated into the final version, which will serve as the official reference document for the protection of Bhutan's Critical Information Infrastructure.

It is expected that the CIIP Baseline document will be finalized by the end of **Week 30** from the start of the assignment. The CIIP Baseline must be developed in close coordination with the G-SOC Handbook, as previously noted (see task 3.2.1.3).

3.3.2. Deliverable 2: CIIP Baseline Implementation Work Plan

Following the completion of the CIIP Baseline, the consultancy firm shall develop a comprehensive Implementation Work Plan for the adoption of the baseline across CII operators.

The implementation should be guided by a phased and adaptive approach, recognizing the varying levels of readiness and capacity across CII organizations. Rather than enforcing a rigid one-size-fits-all rollout, the work plan should promote a "soft implementation" model, enabling gradual adoption of the guidelines in line with each organization's current capacity and maturity level. This includes sequencing activities in a way that prioritizes awareness, training, and capacity-building before enforcement and compliance assessments.

Thus, to develop the CIIP Baseline Implementation work plan the consultancy firm is expected to perform the following tasks:

3.3.2.1. Review of the CIIP Documents

Revisit the CIIP Regulation and the CIIP Baseline with a focus on translating its content into a practical implementation plan. Ensure that key planning elements, particularly those related to governance, compliance, and capacity requirements, are sufficiently detailed. Confirm planning assumptions and parameters through targeted engagement with relevant stakeholders. Following the review, the consultancy firm will address two critical enablers for CII protection: (i) human resources and capacity requirements, and (ii) technical tools and security measures. These tasks will ensure that the Implementation Plan is grounded in both institutional capabilities and the technical infrastructure required for effective CIIP execution.

3.3.2.2. Human Resources and Capacity Requirements

Assess the staffing, expertise, and certification needs required for the effective implementation of CIIP across designated CIIs. Recommend appropriate awareness-raising activities, training programs, and capacity-building initiatives, to strengthen readiness and compliance. This task will be carried out in close consultation with BtCIRT and other relevant stakeholders identified by them. Findings and recommendations will be integrated into the CIIP Baseline Implementation Plan to ensure that human resource and institutional capacity dimensions are fully addressed. It is expected that the Human Resources and Capacity Requirements will be finalized by the end of **Week 34** from the start of the assignment.

3.3.2.3. Technical Tools and Security Measures Specification

Draft the technical specifications for the tools and security measures required to effectively implement and comply with the CIIP Baseline requirements across designated CIIs. This task will include assessing technical needs, defining the required technical specifications, and mapping them against international good practices. This task will be carried out in close consultation with BtCIRT and other relevant stakeholders identified by them. The output of this task will be a detailed technical specification document to inform future procurement processes. The specifications developed under this task will inform the Implementation Plan by providing the basis for a procurement roadmap, including guidance on sequencing and timing, distribution of procured systems across designated CIIs, installation and integration plans, and related support requirements.

It is expected that the Technical Tools and Security Measures Specification will be finalized by the end of **Week 36** from the start of the assignment.

Building on this foundation, the consultancy firm will then proceed to develop rollout plans organized into three main implementation phases, each building on the previous and adapted to the capacity and maturity of individual CIIs: Each phase requires a distinct set of activities, support mechanisms, and timelines, as outlined in the tasks below. It should be noted that the phases may overlap.

3.3.2.4. Phase 1: Introduction

This phase will focus on preparing CIIs for implementation through awareness-raising and foundational capacity development. The consultant shall:

- Define and sequence introductory activities, including workshops, sector-specific briefings, and simulation exercises.
- Outline the development and delivery methods for these awareness initiatives.
- Identify sector-specific technical training needs, including skills gaps.
- Propose capacity assessment mechanisms to evaluate each CII's readiness to proceed with implementation.
- Integrate these training activities into the broader rollout timeline to support long-term institutional development.

3.3.2.5. Phase 2: The Soft Implementation

This phase focuses on supporting the operational adoption of the CIIP Baseline by CIIs through a flexible, staged approach, and is expected to last up to two years. The consultant shall:

- Define a phased implementation strategy that accounts for each operator's initial level of compliance and institutional maturity.
- Propose rollout sequences, timelines, and support mechanisms, ensuring that the approach is risk-informed and context-specific.
- Recommend measures such as technical assistance, procurement support, and tailored guidance to bridge capacity gaps.
- Design a methodology for ongoing monitoring and gap identification during implementation, including options for corrective actions.
- Ensure the plan allows CIIs to progress at their own pace while maintaining overall accountability for compliance milestones.

3.3.2.6. Phase 3: Compliance Monitoring and Review

This phase outlines how compliance with the CIIP Baseline will be assessed and maintained. The consultant shall:

- Translate the compliance provisions from the CIIP Regulation and Baseline into practical monitoring activities, timelines, and institutional responsibilities.
- Design the framework and tools for self-assessments, external audits, and periodic reporting.
- Define oversight roles, escalation procedures, and performance indicators.
- Recommend mechanisms for continuous learning and iterative improvement, ensuring the implementation process remains adaptive and responsive to evolving threats and technologies.

3.3.2.7. Develop Implementation Safeguards

Prepare risk management and M&E processes as safeguards to support effective and adaptive implementation of the CIIP Baseline work plan.

3.3.2.8. Validation of the Draft Implementation Plan

Present the draft CIIP Baseline Implementation Work Plan to key stakeholders for feedback and validation, ensuring alignment with institutional expectations, operational realities, and ACCESS timelines and frameworks. This may be done through a dedicated workshop or a series of structured consultations. Feedback will be incorporated into the final version of the work plan.

Each phase of the plan will require separate approval by BtCIRT, and the consolidated Implementation Work Plan, integrating all phases, safeguards, and interdependencies, will be submitted for BtCIRT's approval by the end of **Week 40** from the start of the assignment.

3.3.2.9. Support for Procurement Preparation

Support the preparation of a Terms of Reference (ToR) for the implementation firm, in accordance with the World Bank's procurement procedures. This includes drafting the technical content of the ToR based on the finalized work plan and outlining the required deliverables, timelines, expertise, and technical specifications. Participate in weekly meetings dedicated to the drafting of ToR not exceeding a period of 3 months.

4. DURATION OF THE ASSIGNMENT

The assignment's implementation is expected to take 40 weeks from the commencement date.

5. SCHEDULE FOR COMPLETION OF TASKS

5.1. Workstream 1: Establishment of the G-SOC

5.1.1. Deliverable 1: G-SOC Handbook

#	Milestone	Description	**Due By** (From the date of contract effectiveness)
1	Inception Report	Detail methodology, work plan, and team structure	Week 4
2	Desk research and review of Background Materials	Review existing documentation including G-SOC Comparative Review Note and the G-SOC Institutional	Week 6
3	Development of initial draft of the G-SOC Handbook	It should include Operational Framework and SOPs; Human Resources and Capacity Requirements; and Technical	Week 18
4	G-SOC Handbook Validation	Conduct a detailed, section-by-section review of the draft report with BtCIRT	Week 30

5.1.2. Deliverable 2: G-SOC Establishment Work Plan

#	Milestone	Description	**Due By** (From the date of contract effectiveness)
1	Development of initial G-SOC Implementation Workplan	The document should include the phases of G-SOC establishment and break them down into actionable	Week 26

2	Development of the G-SOC Implementation Workplan (First Draft)	This deliverable will operationalize the conceptual design into a concrete, time-bound, and costed implementation roadmap.	Week 30
3	Development of G-SOC Technical Design and Specifications	Define all infrastructure, tools, and system requirements necessary for the establishment of the G-SOC.	Week 30
4	G-SOC Skills Development Plan	To be based on the expertise and roles defined in the G-SOC Handbook	Week 30
5	Validation of the Draft Implementation Plan	Present to key stakeholders for feedback and validation	Week 34

5.1.3. Training and Capacity Building on the G-SOC Handbook

#	Milestone	Description	Due By (From the date of contract effectiveness)
1	Preparatory work	(i) Prepare a training plan; (ii) Develop training materials, including presentations, manuals, case studies, and reference documents (as per requirement).	Week 38
2	Conduct the training	(i) Conduct interactive training sessions; (ii) Facilitate knowledge-transfer sessions focused on real-life implementation scenarios; (iii) Any other activities as per requirement of the training objectives.	Week 40

5.2. Workstream 2: Development of CIIP Baseline

5.2.1. Deliverable 1: Development of the CIIP Baseline

#	Milestone	Description	Due By (From the date of contract effectiveness)

1	Outline of CIIP Baseline Components	Drafted from desk review and consultations; forms basis of Operationalization Note.	Week 2
2	CIIP Baseline Operationalization Note	Details methodology, sequence, scope, responsibilities, and deliverables for CIIP Baseline.	Week 6
3	Development of CIIP Baseline Elements	Draft specific baseline elements (e.g. access control, cryptography, OT/ICS security, etc.) with stakeholder validation.	Rolling (no specific week given per element)
4	First Draft of Consolidated CIIP Baseline	All approved elements compiled into a coherent baseline document.	Week 24
5	Final Validated CIIP Baseline Document	Incorporates feedback from validation workshops and senior RGoB leadership.	Week 30

5.2.2. Deliverable 2: CIIP Baseline Implementation Work Plan

#	**Milestone**	**Description**	**Due By** (From the date of contract effectiveness)
1	Human Resources and Capacity Requirements	Assess staffing, skills, and training needs for CII implementation.	Week 34
2	Technical Tools and Security Measures Specification	Define technical requirements and specs for CIIP implementation.	Week 36
3	Draft CIIP Implementation Work Plan(with Phases 1–3 and safeguards)	Includes awareness-building, phased rollout, and compliance monitoring. To be validated via stakeholder consultations.	Week 40

6. DATA, SERVICES AND FACILITIES TO BE PROVIDED BY THE CLIENT

The following facilities will be made available to the Consultants:

- Materials for desk review:
  - 13th Five-Year Plan
  - ACCESS project design documents
  - National Cybersecurity Strategy
  - Cybersecurity institutional roles and responsibilities framework.

    - Draft CIIP Regulation
    - G-SOC Comparative Review Note
    - G-SOC Institutional Design Note
    - Other relevant legal and policy documents
- Office facilities, including meeting rooms and internet
- Transportation for visits to CII agencies related to the assignment

7. CLIENT'S INPUT AND COUNTERPART PERSONNEL

The Professional and support counterpart personnel to be assigned by the Client to the Consultant's team will be determined during the inception of the project.

8. REPORTING REQUIREMENT & TIME SCHEDULE FOR DELIVERABLES

- The consultancy firm will report directly to BtCIRT under the GovTech Agency.
- Regular coordination meetings and monthly progress updates will be required.
- All outputs described in this scope of activities will be reviewed and approved by BtCIRT.

9. PROCEDURE FOR REVIEW OF DELIVERABLES

All required deliverables must be submitted in Docs format, emailed by the identified project manager for the project to the BtCIRT focal/counterpart within the stipulated deadline specified in the timeline in section 5. Any delays and their causes must be communicated well in advance of the expected deadline.

Final acceptance of deliverables will be approved through formal, documented sign-off from the Chief of the BTCIRT, Cybersecurity Division, GovTech Agency.

10. TEAM COMPOSITION & QUALIFICATION REQUIREMENTS FOR THE KEY EXPERTS WHOSE CV AND EXPERIENCE WOULD BE EVALUATED

The consultancy firm must demonstrate proven experience in delivering comparable assignments related to CERT/SOC establishment and CIIP program design in government contexts. The proposed team should combine both policy, technical and operational expertise. The firm may propose individual experts or a mix of in-house and associate experts, ensuring that all required areas of expertise are available throughout the assignment. The team composition provided below shall serve as a minimum baseline requirement, additional experts may be proposed, and more than one expert may be proposed for the same role.

Team Composition:

The table below summarizes the key experts required along with the time inputs required from the experts:

Sl. No.	**Key Experts**	**Numbers**	**Time Inputs in man-months** (from total project timeline of 40 weeks)
1.	Team Leader/Project Manager	1	6
2.	G-SOC Design and Operations Expert	1	7

3.	Capacity Building / Skills Development Expert	1	5
4.	Governance, Crisis Management & Supply Chain Expert	1	4
5.	Senior Cybersecurity Engineering & Controls Expert	1	5
6.	Cloud & Emerging Technologies Security Expert	1	2
7.	OT/ICS Security Expert	1	2

Details of Key Experts:

1) Team Leader / Project Manager - Oversee the overall implementation of the assignment and ensure timely delivery of outputs. Lead the CIIP Workstream and supervise the GSOC Workstream Lead, to ensure methodological consistency, and manage coordination with BtCIRT and CIIs. Lead reporting, workshops, and quality assurance of deliverables. Develop detailed implementation and work plans for the G-SOC and CIIP Baseline, including sequencing, resource estimation, and risk-management planning.

Qualifications:

- Master's degree in Cybersecurity, ICT Management, Project Management, Business Administration, or a related field.
- Certifications such as PMP, PRINCE2, CISSP, or CISM are preferred.

Experience:

- Minimum 10 years of experience managing large-scale cybersecurity or ICT infrastructure projects, including at least one project involving national-level SOC and/or CIIP development.
- Excellent verbal and written communication skills and demonstrated leadership in coordinating multi-stakeholder engagements.
- Experience advising governments or public sector entities preferred.
- Experience coordinating multi-stakeholder engagements.

2) G-SOC Design and Operations Expert - Deliver Workstream 1: G-SOC conceptualization, design, and establishment planning; define G-SOC architecture, and operational framework. Support the development of the TOR for implementation firm as described in 3.2.2.6. Conduct knowledge transfer of GSOC establishment plan to BtCIRT officials through training and capacity development workshop as described in Section 3.2.3.

Qualifications:

- Bachelor's degree in Cybersecurity, Information Systems, Engineering, or a related field.
- Certifications such as CISM / GIAC Security Operations Certified / GIAC Cyber Threat Intelligence (GCTI) are preferred.

Experience:

- Minimum 8 years of experience designing, implementing, or operating national or governmental SOCs/CERTs.
- Familiarity with SOC tools, services, and operational processes.
- Familiarity with both enterprise and open-source SOC solutions.
- Experience in integrating SOC solutions.
- Demonstrated experience in designing or recommending training and certifications for multi-tiered SOC teams.
- Experience advising governments or public sector entities preferred.
- Experience coordinating multi-stakeholder engagements.
- Experience in designing multi-tenant SOC solutions preferred.
- Excellent verbal and written communication skills.

3) Capacity Building / Skills Development Expert - Define staffing, cyber workforce and capacity development requirements for the development and implementation of the G-SOC and CIIP Baseline. Design the capacity-building elements of the CIIP Baseline and any other training or workforce-development components to be included in the CIIP Baseline, as described in Section 3.3.2.2.

Qualifications:

- Bachelor's degree in education, Human Resources, Cybersecurity, Information Systems, Organizational Development, or a related field.
- Certification in training design or adult learning, and certification related to cybersecurity workforce frameworks (e.g., NIST NICE, SFIA), preferred.
- Minimum 8 years of experience in cybersecurity training, workforce development, or institutional capacity building.
- Experience developing curricula or training programs for critical sectors or government entities preferred.
- Experience advising governments or public sector entities preferred.
- Excellent verbal communication skills.

4) Governance, Crisis Management & Supply Chain Expert:
Develop the elements listed below and any additional relevant elements to be included in the CIIP Baseline, as described in Section 3.3.1.1. Support the development of the TOR for implementation firm as described in 3.3.2.9.

Elements to be covered:

1. National Cybersecurity Crisis Management Plan.
2. Third-Party and Supply Chain Security Policy.

Qualifications:

- Bachelor's degree in Cybersecurity, Information Security, Public Policy, or related field.
- Master's degree in Cybersecurity/National Security (preferred).
- Professional certifications preferred: CISSP, CRISC,CISM, CGEIT, ISO 22301 or equivalent.

- Knowledge of national cyber strategies, critical infrastructure protection, and risk governance frameworks.

Experience:

A. 8 plus years of experience in cybersecurity governance, policy development, or national cyber programs.
B. Demonstrated experience developing incident response or crisis management frameworks at national/sectoral level.
C. Experience designing or evaluating third-party/supply chain risk frameworks.
D. Experience conducting cyber workforce planning, skills gap assessments, or cyber capacity development.
E. Experience working with government, national CERT/CSIRT, or critical infrastructure sectors.

5) Senior Cybersecurity Engineering & Controls Expert:

Develop the elements listed below and any additional relevant elements to be included in the CIIP Baseline, as described in Section 3.3.1.1.

Elements to be covered:

- Asset Management baseline
- Access Control and Identity Management baseline
- Cryptography and Data Protection baseline
- Network Security and Threat Detection baseline
- System hardening and configuration/patch management baseline

Qualifications:

A. Bachelor’s degree in Cybersecurity, Computer Science, or Information Technology Engineering.
B. Professional certifications preferred: CISSP/CCNP Security, CySA+, RedHat/Microsoft Security.
C. Strong understanding of enterprise security architecture and technical security controls.

Experience:

- 10 plus years of hands-on experience in multiple security domains including IAM, network security, and data protection.
- Demonstrated experience in developing or implementing:
  - Asset inventories
  - IAM models (RBAC/ABAC, PAM)
  - PKI, key management, encryption standards
  - Network segmentation, firewalls, IDS/IPS
  - SIEM/SOC detection use cases
  - Hardening baselines (CIS, STIGs)
  - Patch management processes
- Experience conducting enterprise-level security assessments and defining baseline security controls.
- Ability to integrate controls across IT, cloud, and hybrid environments.

6) Cloud & Emerging Technologies Security Expert:

Develop the Cloud Security and Emerging-Technologies Security elements of the CIIP Baseline and any related elements to be included in the CIIP Baseline, as described in Section 3.3.1.1.

Elements to be covered:

A. Emerging Tech Security Baseline
B. Cloud Security Baseline.

Qualifications:

- Bachelor's degree in Cybersecurity, Computer Science, Telecommunications, or related field.
- Professional certifications preferred: General Cloud security (e.g., CCSP, CCSK) and/or vendor-specific cloud certifications (AWS certified security speciality, Azure Security Engineer Associate, Google Professional Cloud Security Engineer) or equivalent.
- Additional knowledge in emerging tech security (AI/ML, IoT, 5G).
- Familiarity with cloud reference architectures, CSP shared responsibility models, and zero-trust principles.

Experience:

I. 8 plus years in cloud security architecture, cloud governance, or cloud risk management.
II. Experience establishing cloud security baselines (CIS, NIST, ISO, or custom national frameworks).
III. Experience assessing or securing emerging technologies such as AI/ML pipelines, IoT ecosystems, or 5G networks.
IV. Ability to translate technical findings into policy-level recommendations and baseline controls.
V. Experience with secure DevOps pipelines, cloud workload protection, and container security.

7) OT/ICS Security Expert:
Develop the OT/ICS Security element of the CIIP Baseline and any other related elements to be included in the CIIP Baseline, as described in Section 3.3.1.1.

Elements to be covered:

- OT/ICS Security Baseline.

Qualifications:

1. Bachelor's degree in Engineering, Industrial Control Systems, IT, Cybersecurity, or related field.
2. Professional certifications preferred: GICSP, ISA/IEC 62443, ICS410 or equivalent.
3. Strong understanding of industrial automation technologies, SCADA/PLC/DCS systems.

Experience:

- 6 plus years working with OT/ICS systems in industrial environments (especially power and aviation sector).
- Experience conducting OT/ICS cybersecurity assessments, architecture reviews, or baseline development.

- Experience defining segmentation, monitoring, and secure configuration requirements for OT environments.
- Experience collaborating with engineering teams, operators, and national critical infrastructure stakeholders.