HARAMBEE
REPUBLIC OF KENYA

ICT Authority

COUNTRY: KENYA
PROJECT: KENYA DIGITAL ECONOMY ACCELERATION PROJECT (KDEAP)
IMPLEMENTING AGENCY: Information and Communications Technology Authority (ICTA)
PROJECT ID: P170941; Credit Numbers 7289-KE and 7290-KE

TERMS OF REFERENCE

FOR:

Request for Expression of Interest
for
Design and Supervision of the Set-Up and Operationalization of an ICT Security Operations Centre for Government (GovSOC) (Consulting Firm)

Contract No: KE-ICTA-410949-CS-QCBS

Issue Date: 17th September 2024

Closing Date: 2nd October 2024 at 1000hrs EAT

Client:
The Chief Executive Officer,
ICT Authority
Telposta Towers 12th Floor, Kenyatta Ave
PO Box 27150 - 00100 Nairobi Kenya
Tel: +254 20 2089061/ 2211960 Fax: +254 20 2211960
Email: procurement@ict.go.ke , info@icta.go.ke
Website: www.icta.go.ke

DESIGN AND SUPERVISION OF THE SET-UP AND OPERATIONALIZATION OF AN ICT SECURITY OPERATIONS CENTRE FOR GOVERNMENT (GOVSOC)
(CONSULTING FIRM)

1. INTRODUCTION

The Government of the Republic of Kenya (GoK) has received financing in the amount equivalent to US$390 Million equivalent from the World Bank towards the cost of the first phase of the Kenya Digital Economy & Acceleration Project and it intends to apply part of the proceeds to payments for goods, works, non-consulting services and consulting services to be procured under this project.

The project will include the following components as included in the Project Appraisal Document (PAD).

Component 1: Digital Infrastructure and Services: The aim of this component is to increase access to high-speed internet for individuals, industry, and government—the 'foundation of the foundations' of a digital economy and strengthen Kenya's role as regional digital leader—while leveraging investments from the private sector

Component 2: Digital Government and Services: This component will invest in the foundational digital services, platforms, architectures, and policies needed to transform the way the Government communicates and conducts its internal operations.

Component 3: Digital Skills and Markets: This component aims to equip young Kenyans with digital skills and strengthen their abilities to access and compete in domestic and regional markets through supporting skills development, to study mechanisms to improve access to affordable devices and through enhancing the enabling environment for e-commerce to support Kenya's role as a regional digital hub.

Component 4: Project Management: This component will support project implementation, coordination, for the Project Implementation Unit (PIU) within ICTA and capacity building.

Component 5: Contingent Emergency Response Components: This component will be activated in the event of an emergency. The Gok intends to apply a portion of the proceeds of the Credit to cover activities under sub-components 1.5 (Enhancing Regional Digital Integration). The project aims to accelerate digital transformation at the regional level focusing on critical digital enablers that 'future-proof' economic growth and leveraging Kenya's leadership role in the region to facilitate the adoption and implementation of regionally harmonized frameworks for digital integration

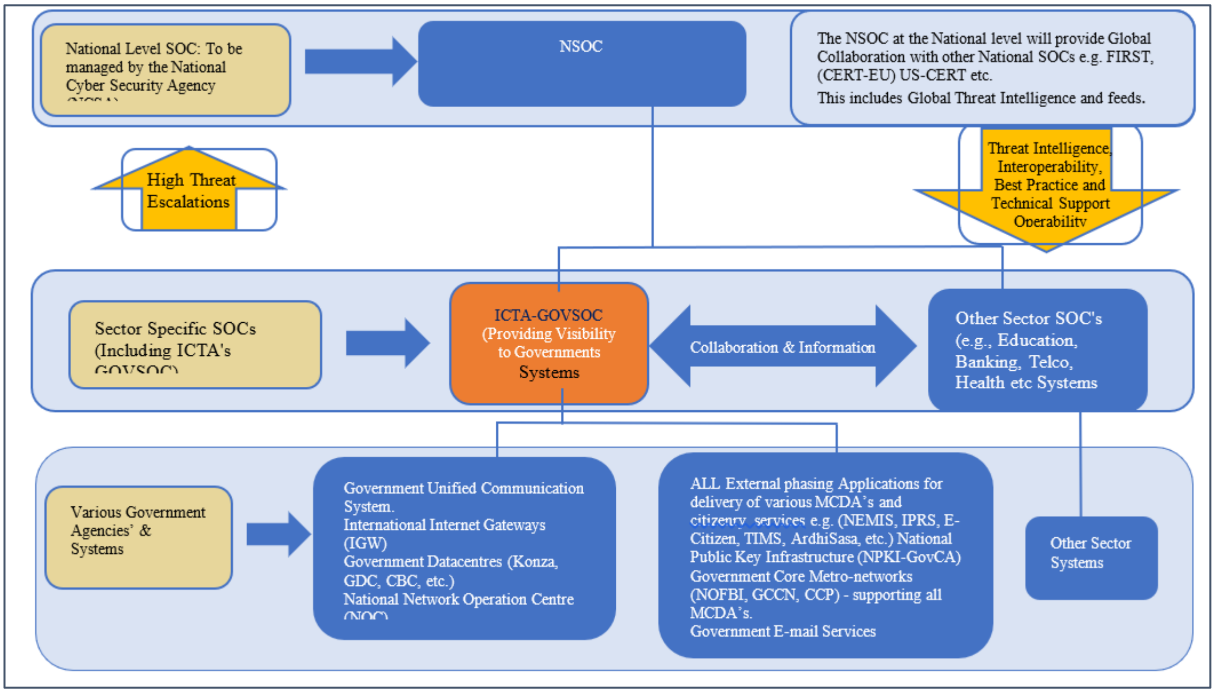
2. BACKGROUND

Over the past decade, the Internet has become increasingly critical for Kenya's economic competitiveness in promoting innovation as well as citizen cantered service delivery in public sector for our collective well-being of Kenyans. We have ported over 15,000 citizen services on the digital platforms all available online. However, this has also led to an increase on Cyber-attacks on Government and critical infrastructures, which constitute a real threat to Kenya's national interest with ICT being a cross-cutting enabler towards the achievement of the Digital Economy. Cyber security is one of the Government's top national security priorities and the Cyber Security Operations Centre is a key part of the deliverable initiative to mitigate these.

Establishing a Government Security Operation Centre (GOVSOC) is not merely a technological infrastructure investment; it's a strategic imperative for ensuring social sustainable economic growth, and the well-being of our citizens in an increasingly connected and digital world. It is an essential step toward building a digitally inclusive and resilient nation.

2.1 THE NATIONAL SOC & GOVSOC HIERARCHY

The Design decision for the Government Security Operation Centre (GOVSOC) shall be based on a hierarchy model with defined authorities for the users. This is as espoused in the Computer Misuse and Cybercrimes Act (2018) and the follow-up Computer Misuse and Cybercrimes Regulations 2024. A multi-tier model of the Security Operations Centre design helps to effectively distribute responsibilities among different sector SOCs, according to the sector requirements, Systems Sensitivity and classification, mandate, skills availability and experience of SOC engineers and the complexity of issues they deal with. The envisaged model for the National SOC and Sector SOC (GovSOC) as depicted below.


National Level SOC: To be managed by the National Cyber Security Agency (NCSA)
NSOC
The NSOC at the National level will provide Global Collaboration with other National SOCs e.g. FIRST, (CERT-EU) US-CERT etc.
This includes Global Threat Intelligence and feeds.
High Threat Escalations
Threat Intelligence, Interoperability, Best Practice and Technical Support Operability
Sector Specific SOCs (Including ICTA's GOVSOC)
ICTA-GOVSOC (Providing Visibility to Governments Systems
Collaboration & Information
Other Sector SOC's (e.g., Education, Banking, Telco, Health etc Systems
Various Government Agencies' & Systems
Government Unified Communication System.
International Internet Gateways (IGW)
Government Datacentres (Konza, GDC, CBC, etc.)
National Network Operation Centre (NOC)
ALL External phasing Applications for delivery of various MCDA's and citizenry services e.g. (NEMIS, IPRS, E-Citizen, TIMS, ArdhiSasa, etc.) National Public Key Infrastructure (NPKI-GovCA)
Government Core Metro-networks (NOFBI, GCCN, CCP) - supporting all MCDA's.
Government E-mail Services
Other Sector Systems

2.2 STRATEGIC USE FOR THE GOVSOC

The Ministry of Information, Communication and The Digital Economy, through the ICTA Authority hosts very Critical Government Infrastructure AND Digital Systems which require round the clock continuous protection, visibility and monitoring to ensure the Government's technology assets and services are not in any way adversely impacted by Cyber threats. Just to name a few, these include;

a) National Public Key Infrastructure (NPKI-GovCA)
b) Government Core Metro-networks (NOFBI, GCCN, CCP) - supporting all MCDA's.
c) Government E-mail Services.
d) Government Unified Communication Platform.
e) International Internet Gateways (IGW)
f) Government Datacentres (Konza, GDC, CBC, etc)
g) National Network Operation Centre (NOC)
h) ALL Government Websites
i) ALL External phasing Applications for delivery of various MCDA's and citizenry services e.g. (NEMIS, IPRS, E-Citizen, TIMS, ArdhiSasa, etc.)
j) Databases, Servers and data centres, and other technologies

The strategic benefits of establishing a Government Systems Security Operation Centre (GOVSOC) are anchored in the four main functions of an ICT GOVSOC which are;

1. To Provide a pro-active Cyber-risk Prevention and detection.
2. To provide a platform for Threats Analysis and Investigation.
3. To Provide a platform for Incidence Response and Management.
4. To Pro-Active Threat Intelligence Sharing
5. To aid in Regional Collaboration on Cyberthreats and IoC, IoA, IoD with our partners.

3. OBJECTIVE OF ASSIGNMENT

The ICT Authority through the World Bank's KDEAP Project seeks the services of a qualified firm to; i) develop a plan ("the Plan") for establishing a Government Systems Security Operation Centre (GOVSOC); and ii) oversite and support the operationalisation of the plan. The Plan will be based on analysis and assessments and will reflect the needs, requirements and objectives of the country and Sector and will detail the services the GovSOC should provide, its design, its target audience, and necessary resources. The Plan should also include a step-by-step roadmap for establishing the GovSOC, as well as relevant procurement documents based on the World Bank's Standard Procurement Documents (SPDs). The Consultant will incorporate widely accepted Good Practices to enable the GOVSOC established through the Plan to participate in international cooperation initiatives and fora (e.g., FIRST). The scope of services, consulting team profiles, reporting requirements and other particulars of the assignment are detailed below.

4. SCOPE OF SERVICES AND SPECIFIC TASKS

4.1 Scope of Services

The scope of services for this assignment will be delivered in two distinct phases: (i) Readiness Study, Development of GOVSOC Implementation plans; and Phase (ii) supervise the establishment and operationalisation of the GOVSOC.

4.1.1 Phase 1: Readiness Study & GovSOC Design

The Consultant is expected to carry out the following tasks:

- **Task 1.1 Prepare for on-site assessment**: The consultant will conduct studies and analysis of the country's current incident response capabilities as well as the broader cybersecurity status. Relevant data and documents can be requested to Country or consulted through desk research if available. This task includes the preparation of a list of relevant stakeholders to be interviewed during the consultation workshops.
- **Task 1.2 Conduct consultation workshops with relevant national and regional stakeholders:** the Consultant will hold a series of interactions and discussions with relevant stakeholders to assess the level of readiness for the creation of a GOVSOC. In this activity the consultant will conduct interviews, ask about the needs, and discuss existing gaps and possible remediation. This task will inform task 3 and 4.

- **Task 1.3 Redact Readiness Assessment Report**: The consultant will prepare a report based on the information collected in Task 1 and 2. The report will provide an overview of the existing incident response capabilities in the country, outline preliminary requirements (e.g., mandate, governance, high-level roadmap, budget) for the GOVSOC establishment plan, and provide insights on the broader cybersecurity context. This report shall include among others:

- GovSOC Needs Assessment:
    - Analyse the government's critical infrastructure and information assets.
    - Assess the current cybersecurity posture and existing security controls.
    - Understand the government's security priorities, threats, and vulnerabilities.
    - Identify stakeholders and their expectations for the GOVSOC.
- GovSOC Gap Analysis:
    - Identify gaps in current security capabilities and how a GOVSOC can address them.
    - Evaluate the need for additional security tools and technologies.
    - Assess staffing needs for the GSOC, Processes and Procedure Implementations including skillsets and expertise required.
- GovSOC Cost-Benefit Analysis:
    - Estimate the costs of establishing and operating a GOVSOC.
    - Analyse the potential benefits of a GOVSOC, such as improved incident detection, faster response times, and reduced risk.
    - Develop a business case for the GOVSOC based on the cost-benefit analysis.
    - Institutional mandate in Cybersecurity, governance and legal considerations
    - Current and recommended ideal GovSOC Governance Structure
    - Recommendation to coordinate the GovSOC in the broader cybersecurity landscape
    - Requirement for GovSOC hosting at the ICT Authority.
    - High-level roadmap and budget requirements
    - High-level requirements for the Design Stage

- **Task 1.4 Redact GOVSOC Establishment Plan**: The consultant will develop a comprehensive plan that defines the services, target audience, necessary resources, and other relevant elements for establishing the GOVSOC at the ICT Authority. The consultant will also provide a step-by-step roadmap for implementing the plan. The Plan shall include among others:

    - Detailed Mandate, governance and legal framework
    - GOVSOC internal policies and procedures
    - GOVSOC Services Plan
    - GOVSOC Processes and Workflows Plan
    - GOVSOC Organisation, Skills and Training Structure Plan
    - GOVSOC Facilities Plan
    - GOVSOC Technologies and Processes Automation Plan
    - GOVSOC Stakeholders Cooperation Plan
    - GOVSOC T IT and Information Security Management Plan
    - A detailed roadmap and Requirements for the Implementation Stage
- Create and submit the requisite technical specifications and documents essential for facilitating an International Competitive Bidding process. This will be in accordance

with the current World Bank Procurement Regulations and will pertain to the anticipated implementation of the ICT GOVSOC.

- Prepare comprehensive draft requirement/specifications tailored for the project. These documents will contain all necessary details and requirements related to the proposed works.
- To prepare a comprehensive schedule outlining detailed cost estimates for the entire project. This schedule will provide a thorough breakdown of expenses associated with different aspects of the installation.
- Prepare an appropriate accompanying training plan that will be executed by the implementation contractor for sustainability and maintenance of the GOVSOC.

All the activities and deliverables mentioned in this ToR shall be completed in conformity with the internationally recognized standards and good practices in GOVSOC deployment.

4.1.2 Phase II: GovSOC Implementation Supervision & Operationalization Support.

The role of the consultant in overseeing the implementation of a Government Cybersecurity Operation centre (GovSOC) will focus on ensuring the project stays on track, meets established goals, and adheres to best practices. The consultant is expected to conducts the following tasks:

- **Task 2.1 Project Management Guidelines:** Provide project management expertise to oversee the implementation of the GovSOC. Develop a project management guideline plan, define milestones, and monitor progress to ensure timely completion of the project.
- **Task 2.2 Vendor/Contractors Management:** Coordinate with vendors, contractors, and suppliers involved in the implementation of the GovSOC. Ensure that they adhere to project specifications, deliverables, and timelines. Review vendor proposals, contracts, and invoices to ensure compliance with project requirements.
- **Task 2.3 Quality Assurance**: Conduct quality assurance checks to verify that the implemented GovSOC aligns with the design specifications.
- **Task 2.4 Risk Management:** Identify potential risks and develop risk mitigation strategies. Monitor and address any issues or challenges that arise during the implementation phase. Implement appropriate risk management measures to minimize disruptions and ensure the successful completion of the project.
- **Task 2.5 Collaboration and Coordination:** Facilitate effective communication and collaboration between different stakeholders involved in GovSOC design and implementation. Coordinate with government departments, IT teams, and other relevant parties to ensure smooth implementation and integration of the GovSOC.
- **Task 2.6 Documentation and Reporting:** Maintain accurate and up-to-date project documentation, including progress reports, change requests, and meeting minutes. Provide regular status updates and progress reports to the government of Kenya, highlighting key milestones, issues, and recommendations.
- **Task 2.7 Compliance and Standards:** Ensure that the implemented GOVSOC design complies with relevant industry standards, regulations, and best practices as highlighted in Annexe 1. Verify that the design and implementation adhere to cyber security guidelines, data protection regulations, and any specific government requirements Kenyan laws & standards, World Bank Operational Safeguard Policies and best practice.

- **Task 2.8 Training and Knowledge Transfer:** Provide training and knowledge transfer requirements and resource needs, and other relevant personnel involved in the operation and management of the GOVSOC.

5. DURATION AND LOCATION OF THE ASSIGNMENT

The duration of the assignment shall be Sixteen (16) months from contract commencement date. The location of the assignment will be in Nairobi, Kenya. The consultant will undertake the task in two phases. The assignment will be for a period of 4 months, in Phase I and 12 months for Phase II. The consultant will proceed with phase II of the assignment on successful delivery of Phase I milestones. The assignment, which will be Lump-sum type of contract for phase1 and Time based for phase II. The consultant will only be invited to proceed with Phase II of the assignment upon approval of the client on successful completion of Phase I, as detailed above and subject to finalization and approval of the designs by the PIU (Project Implementation Unit).

6. REPORTING REQUIREMENTS AND TIMELINES FOR EXPECTED DELIVERABLES

5.1 Phase I (Total duration of 4 months):

The consultant will present the following reports, draft bidding documents and maps:

Table 1: Reporting requirements and timelines for expected deliverables (Phase 1)

OUTPUTS/ DELIVERABLES	DESCRIPTION	TIMELINE FOR SUBMISSION OF DELIVERABLES AFTER CONTRACT COMMENCEMENT	Format of presentation
Inception Report	This report will detail the following; Demonstrate Project understanding, Delivery Methodology and approach in achieving the project objective, communication and risks mitigations, work plan and stakeholders mapping.	3 Weeks	3 hard copies and 1 digital copies
Readiness Assessment Report	The readiness assessment report will provide insights into ICTA's preparedness to establish and deliver the GovSOC. This report will have the current state assessments, that includes people, processes, technology and governance. It will have a gap analysis, the target state description, the implementation roadmap, cost benefit analysis, risks as well as various recommendations.	1 Month.	3 hard copies and 1 digital copies
	The GovSoc establishment plan builds upon the findings of a		

OUTPUTS/ DELIVERABLES	DESCRIPTION	TIMELINE FOR SUBMISSION OF DELIVERABLES AFTER CONTRACT COMMENCEMENT	Format of presentation
GovSoc Establishment Plan	GovSOC readiness assessment report and serves as a roadmap for creating or enhancing a fully functional GovSOC. It will include, introduction, target state definition, design functionality, Staffing plans, technology implementation and GovSOC tools, processes and procedure development as well as training, capacity development and testing and validations and the implementation schedule, sustainability costs and governance.	1.5 Months	3 hard copies and 1 digital copies
Requirements for the GOVSOC establishment and Procurement documents	GOVSOC Requirements and Design Architecture for a Government Security Operations Centre (GSOC) establishment project; along with draft requirement specifications tailored for the project. These documents will contain all necessary details and requirements related to the proposed works.	3 Months	3 hard copies and 1 digital copies
Final Report	The consultant's Final Report will serve as a comprehensive document summarizing the entire GovSOC establishment project. It will showcases the consultant's work and provides a clear picture of the planned Design, establishment supervision for the GovSOC's capabilities. Some of the key findings expected in the documents include; Current Findings and Analysis, GovSOC Design and Functionality, Staff Trainings and requirements, Services , Processes and Procedure Implementations as covered under GAP Analysis.	4 Months	3 hard copies and 1 digital copies

5.2 Phase II (Total duration of 12 months):

The consultant will present the following reports:

Table 2: Reporting requirements and timelines for expected deliverables (Phase II)

OUTPUT REPORT/DELIVERABLE	DETAILS DESCRIPTION	TIMELINE FOR SUBMISSION OF DELIVERABLE FROM DATE OF CONTRACT COMMENCEMENT	NUMBER AND FORMAT OF REPORTS PRESENTATION
Inception Report For Phase II	The Consultant will share the detailed approach, a work plan/ on the Supervision plan, sources of information, staffing and working arrangements necessary to ensure the contractor completes the assignment. The plan should anticipate risk factors and proposed mitigation, sustainability measures based on previous reports	1 Month	3 Hard copies and 1 digital copy
Progress Supervision of Contractor's implementation of GovSOC tools	This supervision report will entail progress report of GOVSOC Tools that are being deployed in the GovSOC.	Monthly	2 Hard copies and 1 digital copy
Final Report	End of Assignment report and delivery of full set of documentation on supervisory works of the GovSOC.	End of Assignment	3 Hard copies and 1 digital copy

The specified copies (1 original copy, 3 hard copies and 1 digital copy) of each of the listed reports shall be sent to the client at the following address:

The Chief Executive Officer,
ICT Authority
Telposta Towers 12th Floor, Kenyatta Ave
PO Box 27150 - 00100 Nairobi Kenya
Tel: +254 20 2089061/ 2211960 Fax: +254 20 2211960
Email: procurement@ict.go.ke , info@icta.go.ke
Website: www.icta.go.ke
Attention:
The Project Coordinator
KDEAP

Upon submission of every report, the consultant is expected to make a presentation of the submitted report to the Client in a scheduled meeting. The acceptance of the report shall be recorded in the minutes of the meeting.

7. PAYMENT SCHEDULE

The proposed payment schedules based on satisfactory performance of the contract which will be negotiated with the successful consultant will be as presented in Table 1 below.

Table 1: Proposed payment schedule (Phase 1) - Lumpsum Contract Payment

S/No.	Deliverables	Timelines after contract commencement	Percentage of the Lump-Sum contract amount
1.	Inception Report	3 Weeks	20%
2.	Readiness Assessment Report GovSoc Establishment Plan	1.5 Months	30%
3.	ToR for the GOVSOC establishment and Bidding documentation	3 Months	20%
4.	Final Report	4th Month	30%

Proposed payment schedule (Phase II) - Time based Contract

The Client shall pay to the Consultant (i) remuneration that shall be determined based on time actually spent by each Expert in the performance of the Services after the date of commencing of Services or such other date as the Parties shall agree in writing; and (ii) reimbursable expenses that are actually and reasonably incurred by the Consultant in the performance of the Services.

Upon submission of every report, the consultant is expected to make a presentation of the submitted report to the Client in a scheduled meeting. The acceptance of the report shall be recorded in the minutes of the meeting.

8. MINIMUM REQUIREMENTS FOR CONSULTANT'S QUALIFICATIONS AND EXPERIENCE

The consulting firm will be required to have a multi-disciplinary team including legal, policy and regulatory experts with deep knowledge and experience in the Kenyan legal, institutional, regulatory and Technology ecosystem. The minimum requirements for the consulting firm qualifications and experience are as follows:

1) **Core business and years in business**: The consulting firm shall be registered/incorporated as a consulting firm with core business in the field of Cybersecurity or related fields for a minimum period of ten (10) years.
2) **Relevant experience:** The firm shall demonstrate as having successfully executed and completed at least two (2) assignments of similar nature and complexity and in a similar operating environment in the last five (5) years. Details of similar assignments, with the name and address of the client, scope, value, and period should be provided and submitted.
3) **Technical and managerial capability of the firm:** The firm shall demonstrate as having the requisite technical capacity and managerial capacity to undertake the assignment in the submitted company profile(s).

9. TEAM COMPOSITION AND MINIMUM QUALIFICATION AND EXPERIENCE REQUIREMENTS FOR THE KEY EXPERTS -PHASE I

The consulting firm shall have well qualified and experienced professionals as required and appropriate for completion of the exercise. They should possess necessary resources to undertake services of such nature including equipment and software required to execute the assignment. The key professionals/expert shall personally carry out (with assistance of other non-key experts and staff deemed appropriate) the services as described in this TOR. The key experts to be provided by the Consulting firm to conduct this assignment for both Phases I are as follows:

No.	Key Experts Education, General Experience & Specific Work Experience
1)	**The Team Leader: (1)** • A minimum of Master's degree in computer science, Cybersecurity, Science Technology, Engineering/ICT, Telecommunications, Electrical Engineering or other relevant fields. • Minimum of 10 years general experience working with government agencies on security matters in Developing and implementing ICT Policy • Minimum of 8 years of specific experience in Cybersecurity program management experience for a government level clientele and have completed works in a similar role. • Certification in Project Management (PMP), Prince 2 Certification or any Other.
2)	**Threat Intelligence Specialist (1):** • A minimum of Master's degree in computer science, Cybersecurity, Science Technology, Engineering/ICT, Telecommunications, Electrical Engineering or other relevant fields. • 8 years general experience in design and implement incident response policies, procedures, workflows and an understanding of SOC Frameworks such as Forum of Incidents Response and Security Teams (FIRST) service framework, National Institute of Standards and Technology (NIST) SP 800-61, ISO/IEC 27035, Systems Admin & Network Security (SANS) Incident Handling Guidelines and their application to building and operating effective Computer Incidents Response teams (CIRTs) • 6 years specific experience in threat intelligence collection, analysis, and dissemination which includes knowledge of Open-Source Intelligence (OSINT) techniques, commercial threat feeds, and malware analysis and knowledge of IR and CIRT establishment frameworks. • Must have at least one certification in Cybersecurity such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk Information Systems Control (CRISC) or GCIH and internationally recognized Security Operation Centre (SOC) auditor certification.
3)	**Security Operations Centre Specialist (1)** • A minimum of Masters degree in computer science, Cybersecurity, Science Technology, Engineering/ICT, Telecommunications, Electrical Engineering or other relevant fields. • 8 years general experience in design and implement incident response policies, procedures, and workflows with a strong understanding of security tools and technologies used in a SOC, such as SIEM (Security Information and

No.	Key Experts Education, General Experience & Specific Work Experience
	Event Management), IDS/IPS (Intrusion Detection/Prevention Systems), firewalls, vulnerability scanners, and malware analysis tools. • 6 years specific experience in SOC Operations Analysis, Threat Hunting, Developing and implementing security monitoring procedures for the government ICT environment and creating and maintaining security dashboards and reports to provide real-time visibility into the security posture of the government network. • Must have at least one certification in Cybersecurity such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk Information Systems Control (CRISC) or GCIH and internationally recognized Security Operation Centre (SOC) auditor certification.
4)	**ICT Security Analysts (1)** • A minimum of Master's degree in computer science, Cybersecurity, Science Technology, Engineering/ICT, Telecommunications, Electrical Engineering or other relevant fields. • 7 years general experience in Developing and implementing security monitoring procedures, Security Incident Response (SIR) procedures for the government, ensuring alignment with best practices. • 5 years specific experience of IT security best practices and frameworks, such as National Institute of Standards and Technology (NIST) Cybersecurity Framework, ISO 27001 and CIS Controls and working experience that entailed Design and Implementation of a comprehensive SOC design, document outlining the tools, technologies, processes, and staffing needs for the SOC. • Must have at least one certification in Cybersecurity such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk Information Systems Control (CRISC) or GCIH and internationally recognized Security Operation Centre (SOC) auditor certification.
5)	**Governance and CII Specialist (1).** • A minimum of Master's degree in Cybersecurity/Information Security, Business/Public Administration, Law, Science Technology, Engineering/ICT, Telecommunications, Electrical Engineering or other relevant fields. • 8 years general experience in Collaborating with government stakeholders to develop a comprehensive security governance framework for the ICT environment. • 6 years specific experience of working in a consulting role with government agencies, with a successful track record of advising clients on ICT security governance and Cybersecurity implementing security programs. • Must have at least one certification in Cybersecurity such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk Information Systems Control (CRISC) or GCIH or Certified Critical Infrastructure Protection Professional (CCIPP).

10. TEAM COMPOSITION AND MINIMUM QUALIFICATION AND EXPERIENCE REQUIREMENTS FOR THE KEY EXPERTS -PHASE II

The consulting firm shall have well qualified and experienced professionals as required and appropriate for completion of the exercise. The table below contains the Qualifications for the Experts in Phase II.

No.	Key Experts Education, General Experience & Specific Work Experience
1)	**The Team Leader: (1)** • A minimum of Master's degree in computer science, Cybersecurity, Science Technology, Engineering/ICT, Telecommunications, Electrical Engineering or other relevant fields. • Minimum of 10 years general experience working with government agencies on security matters in Developing and implementing ICT Policy • Minimum of 8 years of specific experience in Cybersecurity program management experience for a government level clientele and have completed works in a similar role. • Certification in Project Management (PMP), Prince 2 Certification or any Other.
2)	**Threat Intelligence Specialist (1):** • A minimum of Master's degree in computer science, Cybersecurity, Science Technology, Engineering/ICT, Telecommunications, Electrical Engineering or other relevant fields. • 8 years general experience in design and implement incident response policies, procedures, workflows and an understanding of SOC Frameworks such as Forum of Incidents Response and Security Teams (FIRST) service framework, National Institute of Standards and Technology (NIST) SP 800-61, ISO/IEC 27035, Systems Admin & Network Security (SANS) Incident Handling Guidelines and their application to building and operating effective Computer Incidents Response teams (CIRTs) • 6 years specific experience in threat intelligence collection, analysis, and dissemination which includes knowledge of Open-Source Intelligence (OSINT) techniques, commercial threat feeds, and malware analysis and knowledge of IR and CIRT establishment frameworks. • Must have at least one certification in Cybersecurity such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk Information Systems Control (CRISC) or GCIH and internationally recognized Security Operation Centre (SOC) auditor certification.
3)	**Security Operations Centre Specialist (1)** • A minimum of Masters degree in computer science, Cybersecurity, Science Technology, Engineering/ICT, Telecommunications, Electrical Engineering or other relevant fields. • 8 years general experience in design and implement incident response policies, procedures, and workflows with a strong understanding of security tools and technologies used in a SOC, such as SIEM (Security Information and Event Management), IDS/IPS (Intrusion Detection/Prevention Systems), firewalls, vulnerability scanners, and malware analysis tools. • 6 years specific experience in SOC Operations Analysis, Threat Hunting, Developing and implementing security monitoring procedures for the government ICT environment and creating and maintaining security dashboards and reports to provide real-time visibility into the security posture of the government network.

No.	Key Experts Education, General Experience & Specific Work Experience
	• Must have at least one certification in Cybersecurity such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk Information Systems Control (CRISC) or GCIH and internationally recognized Security Operation Centre (SOC) auditor certification.
4)	**ICT Security Analysts (1)** • A minimum of Masters degree in computer science, Cybersecurity, Science Technology, Engineering/ICT, Telecommunications, Electrical Engineering or other relevant fields. • 7 years general experience in Developing and implementing security monitoring procedures, Security Incident Response (SIR) procedures for the government, ensuring alignment with best practices. • 5 years specific experience of IT security best practices and frameworks, such as National Institute of Standards and Technology (NIST) Cybersecurity Framework, ISO 27001 and Centre for Internet Security (CIS) Controls and working experience that entailed Design and Implementation of a comprehensive SOC design, document outlining the tools, technologies, processes, and staffing needs for the SOC. • Must have at least one certification in Cybersecurity such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk Information Systems Control (CRISC) or GCIH and internationally recognized Security Operation Centre (SOC) auditor certification.
5)	**Governance and CII Specialist (1).** • A minimum of Masters degree in Cybersecurity/Information Security, Business/Public Administration, Law, Science Technology, Engineering/ICT, Telecommunications, Electrical Engineering or other relevant fields. • 8 years general experience in Collaborating with government stakeholders to develop a comprehensive security governance framework for the ICT environment. • 6 years specific experience of working in a consulting role with government agencies, with a successful track record of advising clients on ICT security governance and Cybersecurity implementing security programs. • Must have at least one certification in Cybersecurity such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk Information Systems Control (CRISC) or GCIH or Certified Critical Infrastructure Protection Professional (CCIPP).

11. ESTIMATED TIME INPUTS FOR KEY EXPERTS

The number of key experts and the estimated time input for each key expert for the assignment are presented as shown below.

Phase I: Estimated Time Inputs for Key Experts

S/No	Key and support Staff	No	Estimated Time Input (staff-months)
1)	Team Leader	1	4
2)	Threat Intelligence Specialist	1	4
3)	Security Operations Centre Specialist	1	4
4)	ICT Security Specialists	1	4
5)	Governance and CII Specialist	1	4
Total			**20**

Phase II: Estimated Time Inputs for Key Experts

S/No	Key and support Staff	No	Estimated Time Input (staff-months)
1	Team Leader	1	12
2	Threat Intelligence Specialist	1	12
3	Security Operations Centre Specialist	1	12
4	Governance and CII Specialist	1	12
5	ICT Security Specialist	1	12
Total			**60**

12. OBLIGATION OF THE CLIENT

The ICT Authority shall provide the following to the best of its ability as the client the following amenities and facilitation for the consultants in both Phase I & Phase II:

- All background data and literature considered relevant for accomplishing or informing the assignment and completing identified tasks at their immediate disposal.
- Access to key officials and offices within the relevant Ministries/Agencies/department and other relevant official entities, as applicable.
- Facilitate cooperation from other organizations, whose activities and programs may be considered relevant to the assignment.

13. OBLIGATIONS OF THE CONSULTANT

The consultancy must ensure that the tasks identified above are performed in a result-oriented manner with the sole objective of achieving outputs and outcomes expected from the assignment as has been described in the details above. The consultancy is encouraged to utilize local expertise where appropriate.

The Consultant shall be responsible for the provision of all the necessary resources to carry out the services such as international travel, project transportation for visits in counties, subsistence allowances, accommodation, information technology, and means for communications, reporting materials, insurance and any other required resources. The consultant is expected to undertake activities that will ensure that outputs are consistent with the professional and legal requirements. This applies to all Phases – Phase I & Phase II. All outputs will be presented using modern techniques/technology. It is also required that the data is generated through a consultative process that guarantees authenticity and ownership.

END OF TOR