COUNTRY: KENYA
PROJECT: KENYA DIGITAL ECONOMY ACCELERATION PROJECT (KDEAP)
IMPLEMENTING AGENCY: The 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 CONSULTING SERVICES FOR VULNERABILITY ASSESSMENT FOR NATIONAL ICT CYBER SECURITY RISK AND CRITICAL INFORMATION INFRASTRUCTURE.

Contract No: KE-ICTA-411692-CS-QCBS

Issue Date: 11th March 2025

Closing Date: 27th March 2025 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

1. BACKGROUND

The Government of the Republic of Kenya (GoK) has received financing in the amount equivalent to US$390 Million 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).

1. **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
2. **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.
3. **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.
4. **Component 4:** Project Management: This component will support project implementation, coordination, for the Project Implementation Unit (PIU) within ICTA and capacity building.
5. **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

The Government of Kenya gazette Systems and services designated and or classified as Critical Services within the ICT and the Telecommunications Sector. This gazettement encompasses the following categories of systems; Voice and Data communication Systems, Internet Connectivity Systems, Domain and IP Management Systems, Data and Information Management Systems, Encryption Algorithms and Frequency Management Systems.

The ICTA Authority hosts Critical Government Infrastructure & Digital Systems amongst the above defined systems. Just to name a few, these include but not limited to;

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 Datacenters (Konza, GDC, CBC, etc.)
g) National Network Operation Centre (NOC)
h) ALL Government Websites

i) Databases, Servers and data centers, and other technologies

As a country it is important to have a set of guidelines, standards, and best practice principals designed to improve our country's cybersecurity posture and guide various Institutions and agencies on what initiatives and activities need to be done to enhance our Cyber resilience and its maintenance.

While Kenya has taken commendable strides towards enhancing its cybersecurity posture that includes the development of our second National Cyber Security Strategy (The 2022 National Cybersecurity Strategy), important inputs and deliverable and pieces remains the missing puzzles namely: A review, development and enhancement of the National Information Security Framework (NISF), Development of a Cyber Resilience Posture Monitoring and Scoring Framework for CIIs and MDAs, and the Development of a Cybersecurity Audit and Evaluation Toolkit.

These activities are an important aspect to our country's success in its digitization agenda. They foster trust among citizens, businesses and international partners by ensuring the security and privacy of data. This trust is crucial for citizens to embrace digital services, businesses to invest confidently and international collaboration to flourish. NISF also provides the foundation for secure and reliable digital services by guiding the development of secure systems, protecting critical information and ensuring data privacy. This enables the growth of e-commerce, facilitates innovation and streamlines government operations, driving economic growth and improving efficiency.

A National Information Security Framework plays a vital role in national security by safeguarding critical infrastructure, countering cyber threats, and maintaining national sovereignty in the digital realm. In essence a strong NISF is not merely a technical framework; it's a strategic imperative that underpins a nation's digital transformation, fostering a secure, trusted, and resilient digital ecosystem.

2. OBJECTIVE OF THE ASSIGNMENT

The ICT Authority through the KDEAP project seeks to hire a qualified consulting firm to carry out a General ICT Security risk Assessment on the National Threat Landscape and develop the National Information Security Framework (NISF). The NISF will define, among others, the minimum information security controls for Ministries, Departments and Agencies (MDAs) and the national cybersecurity compliance and audit framework for public sector institutions.

3. SCOPE OF SERVICES AND SPECIFIC TASKS OF THE ASSIGNMENT

3.1 Scope of Services

The Consulting Firm shall be required to interact with various players/stakeholders within the Ministry of ICT & The Digital Economy, The ICT Authority, The NC4 and any other relevant stakeholders deemed necessary to provide vital input into this assignment. The ICT Authority is the lead agency and coordinator for this assignment. The assignment will focus on the following:

a) Review and Development of a National Information Security Framework (NISF)
b) Development of a Cybersecurity Audit and Evaluation Toolkit
c) Development of a Cyber Risk Assessment Framework for MDAs
d) Development of a Threat Analysis Framework for the Government CIRT and SOC
e) Pilot Testing of Standards and Certification Framework

3.2 Specific Tasks of the Assignment

The firm will conduct the following FIVE key tasks:

a. **Review and Development of a National Information Security Framework (NISF)**
   i. Develop Kenya's NISF to align with evolving cybersecurity threats, global best practices and regulatory requirements.
   ii. Introduce maturity levels assessment for continuous improvement and a statement of applicability for organizations to tailor controls.
   iii. Incorporate security controls for Critical Information Infrastructure (CII), Operational Technology (OT), APIs and Cloud Hosting.

b. **Development of a Cybersecurity Audit and Evaluation Toolkit**
   i. Create a structured cybersecurity audit and evaluation toolkit based on NISF.
   ii. Ensure the tools' alignment with ISO 27001, NIST 800-53 and other international cybersecurity audit frameworks.
   iii. Provide checklists that is evidence-based audit guidance and templates for conformity assessments for MCDAs.
   iv. Development of a Cyber Resilience Posture Monitoring and Scoring Framework for CIIs and MDAs a methodology for benchmarking CIIs and MDAs against best practices and industry standards (e.g. NIST CSF,CIS Controls,ISO27001,ITU Global Cybersecurity Index).

c. **Development of a Cyber Risk Assessment Framework for MDAs**
   i. **Understanding the Operational and Threat Environment:** The consulting firm shall conduct stakeholder consultations with MDAs to assess cybersecurity challenges and existing risk management practices. This includes analyzing sector-specific cyber risks, regulatory requirements, and identifying key risk categories such as operational, compliance, reputational, and national security risks.
   ii. **Defining Risk Assessment Methodology**: A standardized risk assessment methodology shall be developed, incorporating risk identification and classification criteria, risk impact and likelihood scoring models, techniques for assessing inherent and residual risks, and risk mitigation and treatment strategies. The methodology should align with international standards such as the NIST Cybersecurity Framework, ISO 27005, and COBIT.
   iii. **Developing Risk Assessment Tools and Templates:** Structured risk assessment templates shall be designed to ensure consistency across MDAs. The consulting firm shall also develop a centralized risk registry to track cyber risks within government institutions and provide guidelines for integrating cyber risk assessment into organizational risk management processes.
   iv. **Implementation and Capacity Building** The firm shall provide training and workshops for MDAs on the use of the risk assessment framework. In addition, implementation guidelines should be developed to facilitate integration into strategic decision-making and investment planning. The framework will be piloted with selected MDAs, and refinements will be made based on feedback.

d. **Development of a Threat Analysis Framework for the Government CIRT and SOC**
   i. **Assessing the National Threat Landscape**: The consulting firm shall conduct an in-depth threat landscape analysis to identify prevalent cyber threats targeting national CIIs and government agencies. This will include mapping threat actors such as nation-state actors, hacktivists, cybercriminals, and insider threats.

Historical cyber incidents should be analyzed to identify attack patterns and trends.

ii. **Defining Threat Intelligence and Analysis Methodologies**
The firm shall establish methodologies for structured threat modeling, utilizing frameworks such as MITRE ATT&CK. Key areas of focus will include the identification of Indicators of Compromise (IoCs), threat attribution techniques, and tactical, operational, and strategic threat intelligence analysis to enhance the CIRT's capabilities.

iii. **Designing a Threat Monitoring and Reporting Framework**
A standardized process for cyber threat intelligence collection, analysis, and dissemination shall be developed. This includes the establishment of real-time threat monitoring procedures to enhance proactive detection and the development of reporting templates for intelligence briefs, alerts, and threat advisories for government stakeholders.

iv. **Integration with SOC and Incident Response Processes**
The consulting firm shall define mechanisms for integrating threat analysis with existing Security Operations Centers (SOCs) and Incident Response Teams (IRTs). Playbooks for responding to identified threats will be developed, based on severity and potential impact. Information-sharing protocols should be established to facilitate collaboration with national and international cybersecurity partners.

v. **Capacity Building and Knowledge Transfer**
Training sessions shall be conducted for CIRT analysts on the implementation of the developed threat analysis framework. Operational guidelines should be created to ensure the effective use of threat intelligence in decision-making. The consulting firm shall also provide ongoing advisory support during the initial phase of implementation.

e. Pilot Testing of Standards and Certification Framework

i. Conduct pilot assessments with five MDAs and five CIIs to test the effectiveness of the developed cybersecurity standards.

ii. Provide detailed feedback on implementation, effectiveness, and practicality of the developed standards.

iii. Propose capacity-building initiatives based on pilot findings.

4. DURATION AND LOCATION OF THE ASSIGNMENT

The assignment will be executed within an overall period of Eight (8) calendar months from the contract commencement date. The assignment will be implemented primarily at ICT Authority headquartered in Nairobi, Kenya.

5. REPORTING REQUIREMENTS AND TIMELINE FOR SUBMISSION OF DELIVERABLES

The Consultant is expected to complete the assignment in full within eight (8) months. The Consultant will regularly report to the KDEAP Project Coordinator on all aspects of the agreed activities. The deliverables comprise the following:

Table 1: Requirements and Timeline for Submission of Deliverables.

Outputs/ Deliverables	Description	Timeline for Submission of Deliverables from Contract Commencement date	Format of presentation
Project Inception Report.	This report will provide details of the consultant's understanding of the assignment as well as the methodology and approach to be employed to complete the assignment with clear detailed milestones and work-plan of the exercise implementation as well as Project plan, stakeholder engagement, risk management strategy and resource needs.	**0.5 Months**	Three (3) hard copies and 1 digital copies
Developed/Enhanced NISF: Updated framework with security controls, maturity levels, and applicability guidelines.	For this specific report, the firm will present a developed NISF, incorporating: • **A NISF framework:** A GOK NISF incorporating the latest cybersecurity best practices and addressing identified gaps. This will include; **i.** **Detailed security controls:** Specific and actionable security controls aligned with international standards for each critical area within the framework. **ii.** **Defined maturity levels:** A set of maturity levels (e.g., initial, partial, defined, managed, optimized) to assess the current state of cybersecurity implementation across different sectors. **iii.** **Applicability guidelines:** Clear guidance on how to apply the framework and security controls to different sectors, organizations, and critical infrastructure entities, considering their specific needs and risk profiles. **iv.** **National Threat Landscape Assessment report:** This report will provide an in-depth threat landscape analysis to identify prevalent cyber threats	**2 Months**	Three (3) hard copies and 1 digital copies

Outputs/ Deliverables	Description	Timeline for Submission of Deliverables from Contract Commencement date	Format of presentation
	targeting national CIIs and government agencies. This will include mapping threat actors such as nation-state actors, hacktivists, cybercriminals, and insider threats. Historical cyber incidents should be analyzed to identify attack patterns and trends. This report will provide a comprehensive and practical guide for implementing and maintaining a robust cybersecurity posture across the nation.		
Cybersecurity Audit & Evaluation Toolkit: Guidelines, templates, and conformity assessment methodologies.	The report will contain guidelines, templates, and methodologies for conducting cybersecurity audits and evaluations, including standardized audit procedures, risk assessment frameworks, compliance assessment guidance, reporting standards, and recommendations for remediation. This toolkit aims to provide a consistent and effective approach to cybersecurity assessments, enabling organizations to identify and address their vulnerabilities.	**3 Months**	Three (3) hard copies and 1 digital copies
Development of a Cyber Risk Assessment Framework for MDAs	This report will contain the following deliverables from the Firm; • **An Understanding the Operational and Threat Environment:** This reports on sector-specific cyber risks, regulatory requirements, and key risk categories such as operational, compliance, reputational, and national security risks. • **Defining Risk Assessment Methodology**: The methodology should align with international standards on ISO 27001 • **Developing Risk Assessment Tools and Templates:**	**4.5 Months**	Three (3) hard copies and 1 digital copies

Outputs/ Deliverables	Description	Timeline for Submission of Deliverables from Contract Commencement date	Format of presentation
	• **Implementation and Capacity Building**		
Development of a Threat Analysis Framework for the Government Agencies CIRT and Sector SOCs	The report will provide a comprehensive guidelines for Development of Threat Analysis Frameworks for the Government Agencies' CIRTs and Sector SOCs. This will include; • **Defining Threat Intelligence and Analysis Methodologies.** • **Designing a Threat Monitoring and Reporting Framework.** • **Integration with Sector SOCs and MCDA's Incident Response Processes.** • **Capacity Building and Knowledge Transfer proposal to technical teams for Phase II.**	**6.25 Months**	Three (3) hard copies and 1 digital copies
Pilot Testing of Standards and Certification Framework:	The report will document the findings and recommendations from the pilot testing of the Standards and Certification Framework. It will include: • **Pilot Program Design:** Description of the pilot program, including objectives, scope, selection criteria for pilot participants, and testing methodology. • **Pilot Implementation:** Detailed account of the pilot program execution, including challenges encountered, lessons learned, and best practices identified. • **Evaluation of Standards and Certification Process:** Analysis of the effectiveness, efficiency, and practicality of the standards and certification process based on pilot results. • **Data Analysis and Findings:** Presentation and analysis of data collected during the pilot program, including participant feedback,	**7 Months**	Three (3) hard copies and 1 digital copies

Outputs/ Deliverables	Description	Timeline for Submission of Deliverables from Contract Commencement date	Format of presentation
Evaluation of MDAs and CIIs.	performance metrics, and observations. • **Recommendations for Improvement:** Recommendations for refining the standards and certification framework based on the pilot findings, such as: • Clarifying requirements and procedures. • Addressing identified gaps and inconsistencies. • Improving the ease of use and accessibility of the framework. • Enhancing the efficiency and effectiveness of the certification process. • Next Steps: Recommendations for the next phase of implementation, including a roadmap for full-scale rollout of the framework. This report will provide valuable insights for refining and optimizing the Standards and Certification Framework, ensuring its effectiveness and successful implementation.		
FINAL Project Reports	Executive summary, the key findings, providing all the findings, analysis and deliverables.	**8 Months**	Three (3) hard copies and 1 digital copies

6. PAYMENT SCHEDULE

The proposed payment schedule based on satisfactory performance of the contract which will be negotiated with the successful consultant will be as presented in Table 2 below.

Table 2: Payment Schedule

S/No.	Deliverables	Timeline for Submission of Deliverables from Contract Commencement date	Percentage of the Lump-Sum contract amount
1	Submission and Acceptance of Inception Report	0.5 Months	10%
2	Submission and Acceptance of the Developed/Enhanced NISF: Updated framework with security controls, maturity levels, and applicability guidelines	2 Months	20%
3	Submission and Acceptance of Cybersecurity Audit & Evaluation Toolkit: Guidelines, templates, and conformity assessment methodologies	3 Months	30%
4	Submission and Acceptance of Development of a Cyber Risk Assessment Framework for MDAs	4.5 Months	
5	Submission and Acceptance of Developed Threat Analysis Framework for the Government Agencies CIRT and Sector SOCs	6.25 Months	
6	Submission and Acceptance of Pilot Testing of Standards and Certification Framework: Evaluation of MDAs and CIIs.	7 Months	30%
7	Submission and Acceptance of FINAL Project Reports	8 Months	10%

7. MINIMUM REQUIREMENTS FOR CONSULTANT'S QUALIFICATIONS AND EXPERIENCE

The minimum requirements for the consulting firm's 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 seven (7) 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). **Key experts shall not be evaluated at shortlisting stage.**

8. TEAM COMPOSITION AND MINIMUM QUALIFICATION AND EXPERIENCE REQUIREMENTS FOR THE KEY EXPERTS

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 Consultants to conduct this assignment are as follows:

Table 3: Qualification and Experience Requirements for the Key Experts

No.	Key Experts Education, General Experience & Specific Work Experience
1)	**The team leader: (1)** **Minimum Education Qualification:** • A minimum of Master's degree in computer science, Cybersecurity, Science Technology, Law and/or other relevant fields. • Certification in any of the following: CISSP/CISA/CISM • Project Management certification: Prince 2/PMP **General Experience:** • A Minimum 10+ years of experience in Cybersecurity program management, cybersecurity leadership experience, expertise in strategic planning, governance, and policy development. **Specific Experience:** • Minimum of Five (5) years of experience in developing and implementing security operations strategies for a National government ICT environment with proven experience working with government agencies, critical infrastructure sectors, or regulatory bodies.
2)	**Cyber Risk Management Expert (1 No.)** **Minimum Education Qualification:** • A minimum of Master's degree in Cybersecurity, Computer Science/Technology, Law and/or other relevant fields. • Certification in any of the following: CISSP/CISA/CISM **General Experience:** • A Minimum of 8 years proven experience in threat intelligence collection, analysis, and dissemination. This includes knowledge of open-source intelligence (OSINT) techniques, commercial threat feeds, malware analysis with proven experience in a government environment is a strong plus. **Specific Working Experience:** • A Minimum of 5 years of proven ability to design and implement incident response policies, procedures, cybersecurity frameworks, governance, and compliance development and monitoring.
3)	**Cybersecurity Experts (2 No)** **Minimum Education Qualification:** • A minimum of Master's degree in Cybersecurity/Information Security, IT Technology, or other relevant fields. • Certification in any of the following: CISSP/CISA/CISM

	General Experience: • Minimum of 8 years of experience in planning, implementation, testing, and management of business continuity and crisis response strategies. This includes analysing risks, implementing continuity plans, training staff, or maintaining and updating plans as business needs and environments change. **Specific Work Experience:** • Minimum of Five (5) years' experience with technical expertise in areas like risk assessment, vulnerability analysis, and penetration testing.
4)	**ICT Security Auditor: (2 No)** **Minimum Education Qualification:** • A Minimum of a bachelor's degree in Cybersecurity, Information Technology (IT), Computer Science, or a related field **General Experience:** • A Minimum of 7 years of experience working in a government environment is a strong plus, as it requires an understanding of government security policies, regulations, and compliance requirements. **Specific Work Experience:** • A Minimum of 5 years in implementing or auditing cyber security related standards and/ or frameworks as well as working on ICT and cybersecurity consultancies, projects with documented experience.
5)	**Communications Expert (1 No.)** **Minimum Education Qualification:** • A minimum of Bachelor's degree in communications, journalism, business, advertising, English, or Public Relations). **General Experience:** • Minimum of 7-year experience in creating, implementing and oversight of communications programs, promoting project objectives and ideals. **Specific Work Experience** • A minimum of 4 years specific experience in working with professionals, departments, senior management, and members of the media and press

9. 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 in Table 4.

Table 4: Estimated Time Inputs for Key Experts

S/No	Key and support Staff	No	Estimated Time Input (staff-months)
1)	Firm Lead Consultant/ Team Leader	1	8
2)	Cyber Risk Management Expert	1	8
3)	Cybersecurity Expert	2	16
4)	ICT Security Auditor	2	16
5)	Communications Expert	1	3
Total		6	51 Months.

10. MANAGEMENT AND ACCOUNTABILITY OF THE ASSIGNMENT

The Client for this services is the ICT Authority. The Client will be represented by the Chief Executive Officer (CEO). The Consulting firm will report to the ICT Authority through the KDEAP Project Coordinator as the principal contact for the consulting services.

11. OBLIGATION OF THE CLIENT

The ICT Authority shall provide the following to the best of its ability as the client:

1. All background data and literature considered relevant for accomplishing or informing the assignment and completing identified tasks at their immediate disposal.
2. Access to key officials and offices within the relevant Ministries/Agencies/department and other relevant official entities, as applicable.
3. Facilitate cooperation from other organizations, whose activities and programs may be considered relevant to the assignment.
4. Any required movement from towns within Kenya, workshopping and stakeholder engagements will be considered as a reimbursable.
5. Transport for out of country will be at the cost of the consultant.

12. 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. 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.

13. CONFIDENTIALITY:

The ICT Authority (as the client) and the Consulting firm shall acknowledge and agree that all reports, data, analyses, and other deliverables produced under this Agreement may contain confidential and proprietary information. The Client shall clearly identify any information deemed confidential. The Consultant shall maintain the strictest confidentiality of all such information, use it only for the purposes of this Agreement, and take all reasonable steps to protect its security. The Consultant shall not disclose or use any Confidential Information for any purpose other than as expressly permitted in this Agreement or as required by law.

All information collected and analyzed during the assessment will be treated with strict confidentiality. Where applicable the provisions of the Kenya Official Secrets Act (Cap 197) will be strictly applied and adhered too.