**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:

# EXPRESSION OF INTEREST

# FOR

# IMMEDIATE CLOSURE AND REMEDIATION OF VULNERABILITIES IDENTIFIED IN VAPT OF THE E-CITIZEN PLATFORM

**Contract No: KE-ICTA-526653-CS-QCBS**

**Issue Date: 9th June 2026**

**Closing Date: 24th June 2026 at 10:00AM 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

## BACKGROUND

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.

## 1 INTRODUCTION

The Government of Kenya's eCitizen Platform (www.ecitizen.go.ke) stands as a pivotal digital gateway, facilitating a wide array of e-services and serving as the primary online payment portal for citizens and residents. Launched in 2014, this platform has become an indispensable component of national operations, having processed over 17 million applications and collected more than Kshs 95 billion in revenue. Its critical functions encompass the authentication and legalization of essential documents such as police clearance certificates, academic records, medical reports, birth and death certificates, and marriage certificates. Furthermore, the platform is integral to immigration services, including passport applications, work permits, and various travel passes. This "one login" system is central to

the Government's broader digital transformation agenda, which aims to enhance revenue collection efficiency, reduce operational costs, and improve public service delivery.

The platform's mandate has evolved, with service delivery now coordinated by the Directorate of E-citizen Services under the Ministry of Interior, while payment processing is managed by the Government Digital Payments (GDP) Unit, which falls under The National Treasury, and its ICT Operations are managed by the Ministry of ICT Under ICT Authority.

The E-citizen platform's profound integration into daily civic life and national financial operations means that its integrity and security are matters of national strategic importance. Any compromise or failure could have severe consequences, extending beyond mere service disruption to impact national security, economic stability, and public trust. The substantial financial transactions processed, alongside the highly sensitive personal data handled (e.g., passport information, personal identification details), elevate the stakes significantly.

Recent assessments, including a special audit by the Auditor-General, ICT Authority through a third party VAPT and subsequent parliamentary probes, have brought to light significant vulnerabilities and systemic weaknesses within the E-citizen platform. These findings point to glaring data security deficiencies, alleged financial irregularities, and critical governance gaps.

Beyond data protection, the audit also identified substantial financial discrepancies. These include a reported Sh144 million in missing collections and over Sh1.9 billion in incomplete, duplicated, or improperly reconciled payments. Such findings underscore weak internal controls and limited government oversight over revenue flows. It has also been revealed that the platform's operations are largely controlled by private vendors. This reliance on external entities, coupled with insufficient government oversight, creates a complex operational environment with potential coordination challenges and accountability gaps.

The platform has also been a target of cyber threats. In July 2023, it experienced a Distributed Denial of Service (DDoS) attack that disrupted access to several government portals, exposing its susceptibility to cyberattacks. While government officials have asserted that the platform is under constant surveillance through a Security Operations Centre (SOC) and undergoes regular penetration testing and Data Protection Impact Assessments (DPIAs) , the Auditor-General's findings present a contrasting picture of severe gaps and non-compliance. This apparent contradiction highlights the urgent need for independent verification of existing security controls and a thorough evaluation of their actual effectiveness. The rapid expansion of e-Citizen services, without a corresponding implementation of essential data protection and financial governance mechanisms, poses serious risks to citizen privacy, data security, and the integrity of public funds.

This assignment is therefore imperative to address these identified deficiencies comprehensively. It seeks to ensure the platform's resilience, safeguard citizen data, protect public revenue, and ultimately restore and strengthen public trust in government digital services. The remediation effort

must extend beyond technical fixes to address the underlying governance, compliance, and financial control issues that have been brought to light

## 2. OBJECTIVE(S) OF THE ASSIGNMENT

The Ministry of ICT and Digital Economy through the ICT Authority recently conducted an Independent Third Party Vulnerability Assessment and Penetration Testing (VAPT) of the e-Citizen Platform on behalf of the Government as a Quality Assurance process. The output of the report provided insights into potential classified vulnerabilities that require immediate remediation. The Primary objective of this assignment is to comprehensively remediate all identified significant cybersecurity vulnerabilities within the E-citizen Platform and its associated infrastructure. This effort aims to ensure the platform's integrity, security, and full compliance with all relevant national supporting laws and regulations and standards.

In pursuit of this overarching goal, several secondary objectives have been established;

1. To significantly enhance the platform's overall security posture, bolstering its resilience against current and emerging cyber threats and ensuring continuous service delivery. This involves improving the platform's defensive capabilities and its ability to withstand malicious attacks.
2. To achieve full compliance with the Data Protection Act 2019. This includes facilitating the proper registration of all relevant government entities handling data, establishing a robust and legally sound data protection framework, and formalizing comprehensive data processing agreements with all third-party vendors involved in the platform's operations. This addresses the fundamental legal and governance failures identified in the audit.
3. To establish and operationalize a sustainable, continuous vulnerability management lifecycle for the E-citizen Platform. This framework will incorporate best practices for ongoing identification, assessment, prioritization, remediation, and monitoring of security risks, ensuring that the platform's security posture remains robust over time. This reflects a long-term vision for security, moving beyond a one-off fix to a proactive and adaptive approach.
4. To build internal capacity within relevant government ministries and agencies. This involves equipping personnel with the necessary knowledge and skills for effective cybersecurity management, data protection, and robust vendor oversight concerning critical digital platforms. This focus on internal capability development is crucial for the government to maintain and sustain the enhanced security posture independently in the future.

These objectives collectively aim to address not only the technical symptoms but also the underlying systemic issues related to governance, compliance, and financial management, ensuring a holistic and lasting improvement to the E-citizen platform's security and operational integrity.

## 3. SCOPE OF THE CONSULTING SERVICES AND SPECIFIC TASKS.

The scope of this consulting service assignment encompasses an **end-to-end vulnerability remediation management lifecycle for the E-citizen Platform**. This comprehensive approach mandates that the consultant examines the reported and classified output report from the VAPT exercise, platform components, including integrations, underlying infrastructure (such as servers, databases, network devices, endpoints, software, and security controls), and operational processes. This also extends to components and processes managed by third-party vendors. The assignment must address both technical vulnerabilities and the systemic weaknesses identified in governance, compliance, and financial controls.

### 3.1 SPECIFIC TASKS:

The Consultant shall perform, but not be limited to, the following specific tasks:

#### 3.1.1 Detailed Re-assessment and Validation of Identified Vulnerabilities:

- Conduct a comprehensive asset discovery and inventory across the e-citizen platform components. This includes hardware, software, cloud environments, virtual machines, containers, serverless functions, databases, network components, and third-party tools. The initial step of creating a comprehensive asset inventory is paramount, as a complete understanding of the digital estate is foundational for effective security.
- Execute robust vulnerability scanning and manual testing, including in-depth penetration testing and detailed security assessments, across all identified assets. This is to validate previously identified vulnerabilities and to uncover any new or complex weaknesses that automated tools might have missed. This hands-on approach provides a more nuanced evaluation of the security posture by simulating real-world attacks.
- Analyze the efficiency and effectiveness of existing security controls, such as the Security Operations Centre (SOC), continuous monitoring, and penetration testing mentioned in previous reports. This analysis will identify any discrepancies between reported capabilities and the actual security posture, helping to understand why existing mechanisms may have failed to prevent or detect the identified vulnerabilities.

#### 3.1.2 Prioritization of Vulnerabilities:

- Classify and prioritize all identified vulnerabilities using a structured risk assessment framework. This prioritization will consider:
  - ✓ The criticality and value of the affected assets to government operations and citizen services. Vulnerabilities in key assets, regardless of their inherent severity, often demand immediate attention due to their potential impact.

- ✓ The potential business impact, encompassing financial losses, operational disruption, and legal ramifications. This evaluation ensures that remediation efforts are aligned with the most significant threats to the government's functions.
- ✓ The vulnerability's severity and exploitability, leveraging industry standards such as the Common Vulnerability Scoring System (CVSS) and external threat intelligence (e.g., MITRE's Common Vulnerabilities and Exposures - CVE). This objective scoring helps in focusing on vulnerabilities that are most likely to be exploited.
- ✓ The degree of external exposure of the vulnerability to the internet. Vulnerabilities accessible from the internet typically carry a higher likelihood of exploitation.

- Develop a clear prioritization matrix that will guide remediation efforts. Critical vulnerabilities are to be targeted for immediate action, potentially within 30 days of detection, while high vulnerabilities should be addressed within 60 days.

**3.1.3 Development and Implementation of a Comprehensive Remediation Plan:**

- Design a detailed remediation plan that addresses all identified technical, procedural, governance, and compliance vulnerabilities.
- Implement technical remediation measures, which include but are not limited to:
  - ✓ Deployment of patches and security updates to address known software weaknesses.
  - ✓ Re-configuration of systems and security controls to strengthen defenses.
  - ✓ Implementation of an encrypted architecture, as specifically recommended by the Auditor-General.
  - ✓ Strengthening access controls and network segmentation to limit unauthorized access and lateral movement.
  - ✓ Addressing common application-level issues such as cross-site scripting, inadequate encryption methods, outdated applications, and SQL injections.
- Develop and implement procedural and policy-based remediation measures, including:
  - ✓ Establishing a formal vulnerability management policy that clearly defines processes for identification, assessment, prioritization, remediation, and ongoing monitoring.
  - ✓ Developing and implementing a comprehensive patch management policy.
  - ✓ Defining and implementing strategies for risk acceptance, avoidance, reduction, and sharing for vulnerabilities that cannot be fully remediated immediately or where the cost-benefit analysis dictates alternative approaches.

**3.1.4 Addressing Data Protection Compliance Gaps:**

- Develop and implement a comprehensive data protection framework for the e-citizen Platform, ensuring full alignment with the Data Protection Act 2019. This framework will provide the necessary policies and procedures for lawful and secure data handling.
- Develop and document an Information Security Management System (ISMS) and a Privacy Information Management System (PIMS) tailored for eCitizen operations.

- Draft, review formal written data processing agreements between the Government of Kenya and all third-party data processors (including Webmasters, Pesaflow, Olive Tree Media, and any other relevant entities) involved in the E-citizen Platform. These agreements must ensure strict compliance with the Data Protection Act 2019. This task transforms a legal problem into a concrete implementation requirement, mitigating significant legal and reputational risks.
- Review and enhance existing Data Protection Impact Assessments (DPIAs) processes in conjunction with the ODPC , ensuring they are robust and effectively identify and mitigate privacy risks.

**3.1.4 Strengthening Financial Controls and Reconciliation Processes:**

- Propose for adoption robust internal controls and enhanced oversight mechanisms for revenue flows through the E-citizen Platform. This aims to prevent future financial irregularities.
- Review existing contractual agreements with payment processing vendors (e.g., Pesaflow) to ensure transparency, accountability, and secure handling of public funds.

**4 Post-Remediation Verification, Validation, and Penetration Testing:**

- Conduct independent verification and validation of all implemented remediation measures to confirm their effectiveness in mitigating the identified vulnerabilities.
- Perform follow-up penetration tests and security audits to ensure that vulnerabilities have been fully mitigated and that no new weaknesses have been inadvertently introduced during the remediation process.
- Provide assurance that the platform meets established security benchmarks and compliance requirements post-remediation.

**5 Establishment of a Sustainable, Continuous Vulnerability Management Framework:**

- Design and assist in the implementation of a continuous monitoring and improvement framework for vulnerability management. This ensures that the security posture evolves with new threats and changes to the platform.
- Recommend and assist in the deployment of automated tools for vulnerability scanning, patch deployment, and IT asset management to enhance efficiency and consistency in ongoing security operations.
- Develop clear procedures for regular review and evolution of the vulnerability management process, enabling it to adapt to changes in the organization's technical estate, new threats, and emerging vulnerabilities.

## 3.2 DOWNSTREAM WORK/TASK REQUIREMENTS:

**3.2.1 Policy and Legal Framework Development:** Assist in the drafting or refinement of policies and legal frameworks pertaining to cybersecurity, data protection, and digital payments. This addresses the deeper systemic issues that allowed the vulnerabilities to manifest.

**3.2.2 Inter-Agency Coordination Mechanisms:** Propose and assist in establishing formal coordination mechanisms between the Directorate of E-citizen Services (under the Ministry of

Interior) and the Government Digital Payments Unit (under The National Treasury). This is crucial to ensure unified security governance, operational oversight, and clear lines of authority for the E-citizen platform, addressing the challenges posed by its split functional ownership.

**3.2.3 Vendor Contract Review and Renegotiation:** Conduct a comprehensive review of all existing contracts with third-party vendors (Webmasters, Pesaflow, Olive Tree Media) to identify and address contractual gaps related to data protection, security responsibilities, performance metrics, and financial accountability. Recommendations for renegotiation will be provided where necessary to ensure stronger government control and accountability.

## 3.3 TRAINING AS A SPECIFIC COMPONENT OF THE ASSIGNMENT:

**3.3.1 Capacity Building Workshops:** Conduct comprehensive training workshops for key government IT, cybersecurity, legal, and financial personnel who are involved in the E-citizen Platform's operations and oversight. The training curriculum should cover:

- ✓ Advanced vulnerability management techniques and best practices.
- ✓ Effective utilization of vulnerability management tools and automation.
- ✓ Compliance requirements under the Data Protection Act 2019, with a specific focus on data controller and processor responsibilities and the nuances of data processing agreements.
- ✓ Enhanced financial oversight and reconciliation procedures for digital payments.
- ✓ Incident response and crisis management protocols tailored for critical government digital platforms.

**3.3.2 Knowledge Transfer:** Ensure effective and practical knowledge transfer to designated government counterpart personnel. This will empower them to independently manage and maintain the enhanced security posture of the E-citizen platform post-assignment, fostering long-term self-sufficiency and reducing reliance on external consultants.

## 4. DURATION AND LOCATION OF THE ASSIGNMENT

The assignment is expected to be completed within a period of six (6) Months calendar months from the contract commencement date. The specific duration will be determined based on the comprehensive assessment of the scope and complexity of the identified vulnerabilities and the proposed remediation plan.

The primary location of the assignment will be Nairobi, Kenya. This will specifically involve on-site presence at the offices of The National Treasury, the Ministry of Interior, ICT Authority and potentially at the Security Operations Centre (SOC) located at Nyayo House. Given that the E-citizen platform handles highly sensitive citizen data and substantial financial transactions, and considering the identified governance and oversight issues, direct, on-site presence is deemed crucial. This ensures secure access to systems, facilitates direct interaction with government personnel and vendors, and allows for effective oversight of the consultant's activities. While on-site presence is paramount for collaboration and access to critical systems, secure remote work arrangements may be considered for specific tasks, subject to explicit client approval and strict adherence to all government data security protocols.

## 5. REPORTING REQUIREMENTS AND TIMELINES FOR SUBMISSION OF DELIVERABLES

The Consultant shall submit reports and deliverables in the specified format, frequency, and content. All reports are required in both hard copies and electronic format (USB or secure digital submission), with final reports specifically requiring USB in addition to hard copies. This detailed reporting structure ensures rigorous oversight and accountability throughout the project.

### 5.1 MINIMUM REPORTING REQUIREMENTS:

1. **Inception Report:** This report will detail the proposed work plan, methodology, refined timeline, team mobilization plan, initial assessment findings, and any immediate critical observations. It is due within 15 calendar days from the contract commencement date.
2. **Vulnerability Re-assessment and Prioritization Report:** This comprehensive report will include a detailed asset inventory, findings from vulnerability scans and penetration tests, a validated list of vulnerabilities, a thorough risk assessment, and a prioritized remediation roadmap. This report must clearly articulate critical and high vulnerabilities, along with their recommended remediation timelines (e.g., 15 days for critical, 30 days for high). It is due within 30 calendar days from the contract commencement date.
3. **Interim Progress Reports:** These reports will provide updates on remediation activities, challenges encountered, proposed solutions, an updated risk register, and upcoming activities. They are to be submitted monthly, by the 5th day of each subsequent month.
4. **Data Protection Compliance Remediation Report:** This report will document the formal registration of the GDPU and other relevant government entities with the ODPC, the finalized data protection framework, executed data processing agreements with third-party vendors, and comprehensive evidence of compliance with the Data Protection Act 2019. This dedicated report underscores the critical nature of addressing legal and compliance gaps. It is due within 60 calendar days from the contract commencement date.
5. **Final Remediation Report:** This comprehensive report will provide an overview of all remediation activities undertaken, a detailed description of implemented technical and procedural changes, post-remediation verification results, and an updated security posture assessment. It is due upon completion of all remediation tasks, prior to contract closure.
6. **Post-Remediation Audit and Sustainability Plan Report:** This report will include independent audit findings, detailed recommendations for the continuous vulnerability management framework, the proposed training curriculum, and a long-term sustainability plan for the E-citizen Platform's security. It is due within 15 calendar days after the Final Remediation Report submission.
5. **DESIGNATED RECIPIENTS:**

Reports shall be submitted to the following persons, reflecting the split oversight of the E-citizen platform between the National Treasury and the Ministry of Interior and The Ministry of ICT through ICT Authority.

**Table 1: Report/Deliverable Submission Schedule**

| S.No. | Report/Deliverable | Timelines Of Submission From Contract Commencement Date | Format Of Presentation Of Reports |
|---|---|---|---|
| 1 | Project Inception Report | Within 0.5 Months | Hard copy (4), Electronic (USB/Secure Digital) |
| 2 | Vulnerability Re-assessment & Prioritization Report | Within1(One) Month | Hard copy (4), Electronic (USB/Secure Digital) |
| 3 | Interim Progress Reports | Monthly (by 5th day of subsequent month) | Hard copy (4), USB(Secure Digital) |
| 4 | Data Protection Compliance Remediation Report | Within two (2) Months | Hard copy (4), Electronic (USB/Secure Digital) |
| 5 | A comprehensive gap analysis report against ISO 27001 and ISO 27701 requirements. | Within Three (3) Months | Hard copy (4), Electronic (USB/Secure Digital) |
| 6 | Final Remediation Report | Upon completion of all remediation tasks | Hard copy (4), Electronic (USB/Secure Digital) |
| 7 | Post-Remediation Audit & Sustainability Plan Report | Within 15 calendar days after Final Report submission | Hard copy (4), Electronic (USB/Secure Digital) |

This tabular format provides a clear, visual summary of all key deliverables and their deadlines, which is invaluable for both project management and contractual clarity.

## 6. PAYMENT SCHEDULE/REMUNERATION

The proposed payment schedule shall be based on the successful submission and formal acceptance of key deliverables, reflecting a lump-sum contract approach. The Consultant shall submit invoices upon the formal acceptance of each deliverable by the Client. The strategic phasing of payments aligns with the critical milestones and the comprehensive, phased approach to addressing the various types of vulnerabilities identified.

**Table 2: Payment Schedule**

| S.No. | Deliverable/Milestone | Payment Percentage | Due Date/Trigger |
|---|---|---|---|
| 1 | Upon acceptance of Inception Report | 10% | Within 15 calendar days of contract commencement |
| 2 | Upon acceptance of Vulnerability Re-assessment & Prioritization Report | 20% | Within 30 calendar days of contract commencement |
| 3 | Upon acceptance of Data Protection | 20% | Within 60 calendar days of |

| | | | |
|---|---|---|---|
| | Compliance Remediation Report | | contract commencement |
| 4 | Upon acceptance of gap analysis report. | 20% | Within 90 calendar days of contract commencement |
| 5 | Upon acceptance of Final Remediation Report | 20% | Upon completion of all remediation tasks |
| 6 | Upon acceptance of Post-Remediation Audit & Sustainability Plan Report | 10% | Within 15 calendar days after Final Report submission |
| | **Total** | **100%** | |

## 7. MINIMUM REQUIREMENTS FOR CONSULTANT'S QUALIFICATIONS AND EXPERIENCE

The shortlisting criteria for the consulting firm for this assignment are stringent, reflecting the complexity, national importance, and sensitive nature of remediating vulnerabilities within the E-citizen platform.

- **Core Business and Years in Business:** The firm must be formally registered and incorporated as a consulting firm with a core business demonstrably in cybersecurity, information security, IT governance, risk and compliance (GRC), or an equivalent field. This specialization must have been maintained for a minimum period of **ten (10) years**. This extensive operational history indicates a depth of experience necessary for a project of this magnitude.

- **Relevant Experience:** The firm shall demonstrate having successfully executed and completed at least **five (5) assignments** of a similar nature and complexity. This includes large-scale enterprise cybersecurity remediation, projects involving government digital platforms, or critical national infrastructure. These assignments must have been completed within the last **seven (7) years**. Experience in a similar operating environment is crucial, as government systems often present unique bureaucratic, procurement, and political complexities that differ significantly from the private sector. Detailed information for each similar assignment, including the name and address of the client, the scope of work, value, and period of execution, must be provided with the Expression of Interest.
- **Technical and Managerial Capability of the Firm:** The firm must demonstrate the requisite technical capacity, including access to advanced cybersecurity tools, proven methodologies, and established frameworks. Furthermore, it must exhibit strong managerial capability, evidenced by project management certifications, a robust organizational structure, and rigorous quality assurance processes, all necessary to undertake an assignment of this national significance. This demonstration should be clearly articulated in the submitted company profile(s).
  Key Experts will not be evaluated at the shortlisting stage.

## 11. 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 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)**<br>• A minimum of Master's degree in computer science, Cybersecurity, Science Technology, Engineering/ICT, Telecommunications, Electrical Engineering or other relevant fields.<br>• Minimum of 10 years general experience working with government agencies on security matters in Developing and implementing ICT Policy<br>• 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.<br>• Certification in Project Management (PMP), Prince 2 Certification or any Other. |
| 2) | **Lead Cybersecurity Architect/Engineer (1):**<br>Academic Qualification: A minimum of a Bachelor's degree in Computer Science, Software Engineering, or a related field. A Master's degree is preferred.<br>• General Experience: A minimum of ten (10) years of general experience in IT infrastructure, network architecture, and software development.<br>• Specific Experience: A minimum of seven (7) years of specific experience in designing, implementing, and securing complex enterprise-level systems. This includes expertise in cloud security (e.g., AWS, Azure, GCP security best practices) 8, network security, application security (including addressing issues like SQL injections, cross-site scripting) 9, and secure coding practices. Experience with encrypted architecture implementation 5 is highly desirable.<br>• Professional Certification: Possession of relevant certifications such as Certified Cloud Security Professional (CCSP), Offensive Security Certified Professional (OSCP), or equivalent. |
| 3) | **Data Privacy and Compliance Specialist:**<br>• **Academic Qualification**: A minimum of a Bachelor's degree in Law, Information Systems, or a related field. A Master's degree with a focus on data protection law is preferred.<br>• **General Experience:** A minimum of eight (8) years of general experience in legal or compliance roles within the technology sector.<br>• **Specific Experience:** A minimum of five (5) years of specific experience in implementing data protection frameworks, conducting Data Protection Impact Assessments (DPIAs), drafting and reviewing data processing agreements, and ensuring compliance with data protection regulations, specifically the Data Protection Act 2019 of Kenya.5 Experience with government data handling protocols is a significant advantage.<br>• Professional Certification: Possession of relevant certifications such as Certified Information Privacy Professional (CIPP), Certified Data Privacy Solutions Engineer (CDPSE), or equivalent. |

| No. | Key Experts Education, General Experience & Specific Work Experience |
|---|---|
| 4) | **Financial Systems Security Expert/Auditor:**<br>• Academic Qualification: A minimum of a Bachelor's degree in Accounting, Finance, Information Systems Audit, or a related field. Professional accounting or auditing qualifications (e.g., CPA, ACCA) are preferred.<br>• General Experience: A minimum of ten (10) years of general experience in financial auditing, internal controls, or financial system implementation.<br>• Specific Experience: A minimum of seven (7) years of specific experience in auditing or securing financial systems, payment gateways, or large-scale revenue collection platforms. Demonstrated ability to identify and remediate financial discrepancies and weak internal controls, as highlighted in the Auditor-General's report 5, is critical.<br>• Professional Certification: Possession of relevant certifications such as Certified Information Systems Auditor (CISA), Certified Fraud Examiner (CFE), or equivalent. |
| 5) | **Security Operations Centre Specialist (1)**<br>• A minimum of Master's degree in computer science, Cybersecurity, Science Technology, Engineering/ICT, Telecommunications, Electrical Engineering or other relevant fields.<br>• 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.<br>• 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.<br>• 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. |
| 6) | **ICT Security Analysts (1)**<br>• A minimum of Master's degree in computer science, Cybersecurity, Science Technology, Engineering/ICT, Telecommunications, Electrical Engineering or other relevant fields.<br>• 7 years general experience in Developing and implementing security monitoring procedures, Security Incident Response (SIR) procedures for the government, ensuring alignment with best practices.<br>• 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. |

| 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. |
| 7) | **Vulnerability Management Specialist/Penetration Tester:**<br>• Academic Qualification: A minimum of a Bachelor's degree in Computer Science, Cybersecurity, or a related technical field.<br>• General Experience: A minimum of seven (7) years of general experience in cybersecurity operations or security testing.<br>• Specific Experience: A minimum of five (5) years of specific experience in conducting comprehensive vulnerability assessments, penetration testing, and red teaming exercises for complex enterprise systems. Proficiency in using automated vulnerability scanning tools and conducting manual testing 8 is essential. Experience in validating remediation efforts and continuous monitoring 7 is also required.<br>• Professional Certification: Possession of relevant certifications such as Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH), or equivalent. |
| 8) | **Governance and CII Specialist (1).**<br>• 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.<br>• 8 years general experience in Collaborating with government stakeholders to develop a comprehensive security governance framework for the ICT environment.<br>• 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.<br>• 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). |

## 12. 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 | 6 |

| | | | |
|---|---|---|---|
| 2) | Lead Cybersecurity Architect/Engineer | 1 | 6 |
| 3) | Data Privacy and Compliance Specialist: | 1 | 6 |
| 4) | Security Operations Centre Specialist | 1 | 6 |
| 5) | Financial Systems Security Expert/Auditor: | 1 | 6 |
| 6) | ICT Security Specialists | 1 | 6 |
| 7) | Vulnerability Management Specialist/Penetration Tester: | 1 | 6 |
| 8) | Governance and CII Specialist | 1 | 6 |
| **Total** | | | **42** |

## 13. MANAGEMENT AND ACCOUNTABILITY OF THE ASSIGNMENT

This section delineates the responsibilities of both the Client (Government of Kenya) and the Consultant to ensure effective management and successful execution of the assignment.

### 13.1 Obligations of the Client:

The ICT Authority and related Agencies shall provide the following services, facilities, property, and personnel to the Consultant to facilitate the successful execution of this critical assignment:

1. **Services, Facilities and Property:**
    a) Timely and secure access to all relevant E-citizen Platform documentation, including architectural diagrams, system configurations, existing vulnerability assessment reports, audit findings , and relevant policy documents.
    b) Provision of secure, dedicated office space and necessary utilities (e.g., internet connectivity, power) within government premises (such as The National Treasury, Ministry of Interior, or Nyayo House) for the duration of the assignment.
    c) Provision of secure access to E-citizen Platform systems and environments (development, staging, and production) as required for comprehensive assessment, testing, and remediation activities. This access must strictly adhere to all government security protocols.
    d) Facilitation of prompt meetings with relevant government officials, key stakeholders (including representatives from The National Treasury, Ministry of Interior, Directorate of E-citizen Services, GDP Unit, and the Office of the Data Protection Commissioner), and third-party vendors (Webmasters, Pesaflow, Olive Tree Media). This explicit commitment to facilitating access and meetings acknowledges the need for significant government support to navigate the complex multi-ministry and multi-vendor environment.
2. **Professional and Support Counterpart Personnel:**
    - Assignment of a dedicated Project Liaison Officer from each of the primary ministries (The National Treasury and Ministry of Interior ICT&DE) to facilitate seamless coordination, information sharing, and timely decision-making.
    - Designation of qualified technical, legal, and financial counterpart personnel from relevant

government departments (e.g., IT, cybersecurity, legal, audit, finance) to work collaboratively with the Consultant's team. This arrangement is crucial for ensuring effective knowledge transfer and continuity of operations post-assignment, building internal government capacity for future cybersecurity management.

## 13.2 Obligations of the Consultant:

The Consultant shall adhere to the following stringent obligations throughout the assignment:

1. **Proprietary Rights of Client in Reports and Records:** All reports, raw data, findings, methodologies, tools developed or customized, and any other intellectual property generated during the course of this assignment shall be the sole and exclusive property of the Government of Kenya. The Consultant shall not disclose any information obtained during the assignment to any third party without the express written consent of the Client. This protects the government's legal position and sensitive information.
2. **Adherence to Kenyan Laws and Regulations:** The Consultant shall strictly comply with all applicable Kenyan laws and regulations. This includes, but is not limited to, the **Data Protection Act 2019**, the Public Procurement and Asset Disposal Act, and any other relevant cybersecurity and financial regulations. This strong emphasis on legal compliance is paramount, especially given the identified non-compliance issues within the E-citizen platform itself.
3. **Confidentiality and Non-Disclosure:** The Consultant and all its personnel shall maintain strict confidentiality regarding all information, data, and systems accessed during the assignment. A formal Non-Disclosure Agreement (NDA) will be signed by all relevant parties prior to the commencement of work, reinforcing the commitment to data security.
4. **Compliance with Government Security Policies:** The Consultant shall meticulously adhere to all established Government of Kenya cybersecurity policies, standards, and procedures. This encompasses protocols related to remote access, data handling, incident reporting, and personnel security.
5. **Quality Assurance:** The Consultant shall implement robust quality assurance processes to ensure the accuracy, completeness, and effectiveness of all deliverables and remediation activities, guaranteeing high standards of work.
6. **Ethical Conduct:** The Consultant and its personnel shall conduct themselves with the highest level of professionalism, integrity, and ethical conduct throughout the assignment, maintaining public trust.

**End of TOR.**