PublicPrivate
Partnership
Commission

THE DIGITAL MALAWI ACCELERATION PROJECT

GRANT NUMBER	**:**	**IDA-E338-MW**
PROJECT NUMBER	**:**	**P505095**

TERMS OF REFERENCE

CONSULTANCY SERVICES TO CARRY OUT COMPREHENSIVE VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) FOR GOVERNMENT DIGITAL INFRASTRUCTURE

CONTRACT NO: MW-PPPC-452993-CS-CQS

DATE: MAY 2025

A. BACKGROUND

Information and Communication Technology (ICT) is now globally recognized as an essential tool in promoting competitiveness, job creation, sustainable development, and overall poverty reduction. A combination of widespread access to broadband and a robust ICT services ecosystem can offer a powerful platform for reducing poverty, improving human development, and increasing government transparency and efficiency. ICTs have the potential to transform business and government—driving entrepreneurship, innovation, and economic growth, and breaking down barriers of distance and cost in service delivery.

In recognition of the critical role that ICT plays in fostering socio-economic development and empowering the poor, the Government of Malawi secured funding from the World Bank to implement the Digital Malawi Acceleration Project (DMAP). The line Ministry and owner of the project is the Ministry of Information and Digitalization (MoID), with the Public Private Partnership Commission (PPPC) serving as the lead implementation agency. Other key stakeholders include the Ministry of Education, the Malawi Research and Education Network (MAREN), the National Registration Bureau (NRB), and the Malawi Communications Regulatory Authority (MACRA).

The expansion of the government's digital infrastructure—including the Government Email System, the E-Service Portal (Bomalathu), the DNS System, the National Data Center, and the core network infrastructure—necessitates a proactive cybersecurity approach. To safeguard these critical systems, the Government of Malawi seeks to conduct a Vulnerability Assessment and Penetration Testing (VAPT) to identify, assess, and mitigate security risks.

B. OBJECTIVE

The Government of Malawi is seeking the services of a qualified firm to conduct a Comprehensive Vulnerability Assessment and Penetration Testing (VAPT) on critical government digital infrastructure. The firm will identify, assess, and mitigate security vulnerabilities, providing actionable recommendations to enhance the overall cybersecurity posture of government systems.

The scope of work includes assessing security risks across government networks and systems, conducting penetration testing to simulate cyber threats, developing a risk mitigation and remediation plan, and delivering cybersecurity training to enhance the capacity of government ICT personnel.

C. SCOPE OF WORK

The consulting firm ("Consultant") will conduct a Comprehensive **Vulnerability Assessment and Penetration Testing (VAPT)** on Malawi's critical government digital infrastructure to identify, assess, and mitigate security risks.

More specifically, the Consultant is expected to carry out the following tasks:

1. Conduct a Security Risk Assessment

- Identifying vulnerabilities across internet-facing systems, internal networks, and critical infrastructure.
- Evaluating potential threats, attack vectors, and system weaknesses.
- Mapping security gaps and assessing the likelihood and impact of exploitation.

- Documenting risks with severity classifications and mitigation,

2. **Perform Penetration Testing**
    - Simulating real-world cyberattacks to test system resilience.
    - Executing controlled exploitation to assess security controls.
    - Evaluating authentication, authorization, and access control mechanisms.
    - Reporting on exploitable vulnerabilities with recommendations for remediation.

3. **Develop a Risk Mitigation and Remediation Plan**
    - Providing prioritized remediation steps based on risk assessment findings.
    - Recommending security best practices for infrastructure hardening.
    - Drafting guidelines for secure coding, system patching, and configuration management.
    - Suggesting security tools and policies to strengthen defences.

4. **Deliver Security Training and Knowledge Transfer**
    - Conducting workshops for government ICT personnel on vulnerability management.
    - Training on secure coding, system hardening, and penetration testing techniques.
    - Providing guidance on incident response and cybersecurity best practices.
    - Transferring skills for continuous monitoring and security improvements.

D. EXPECTED DELIVERABLES & SCHEDULE OF COMPLETION

The Consultant is expected to complete the assignment in full within 13 weeks, and to submit the following deliverables, based on the indicative timelines and payment schedule detailed below:

S/No	Milestone/deliverable	Timeline	Indicative payment schedule
D1.	Inception Report, detailing methodology, scope, and work plan for the assignment	Within 1 week of contract signing	10%
D2.	Security Risk Assessment and Penetration Testing Report, identifying vulnerabilities, assessing risks, and evaluating security controls	Within 6 weeks of approval of the Inception Report	30%
D3.	Risk Mitigation and Remediation Plan, outlining prioritized security recommendations, best practices, and corrective measures	Within 2 weeks of completion of the Security Assessment	20%

S/No	Milestone/deliverable	Timeline	Indicative payment schedule
D4.	Training and Knowledge Transfer, covering vulnerability management, penetration testing techniques, incident response, and cybersecurity best practices for government ICT personnel	Within 2 weeks of completing the Risk Mitigation Plan	20%
D5.	Final Report, summarizing key findings, remediation efforts, training outcomes, and recommendations for future security improvements	Within 2 weeks of completing all prior deliverables	20%

E. CONTRACTING, REPORTING AND VALIDATION PROCEEDURE

The Consultant will be contracted by the Government of Malawi, which will oversee payments and approve deliverables. All deliverables must be submitted to the Director of eGovernment for review and final approval. Written deliverables should be provided in both PDF and editable Word formats to allow for comments and necessary edits.

The Consultant will work closely with an assigned Government Cybersecurity Specialist on a daily basis, along with a designated focal point at the Department of e-Government, which will be the primary beneficiary of this assignment. Regular check-ins, validation meetings, and progress updates will be required to ensure alignment with project objectives and expected outcomes.

F. CLIENT'S RESPONSIBILITIES

The Ministry of Information and Digitalization (MoID) and the World Bank (WB) shall provide the following support to the best of their ability:

- Relevant Background Data & Documentation – Provide all available literature, reports, and data necessary to inform and support the assignment.
- Access to Key Stakeholders – Grant access to key officials within relevant Ministries, Agencies, and Departments to facilitate discussions and information gathering.
- Facilitation of Cooperation – Assist in securing collaboration from other organizations whose programs and activities may be relevant to the assignment.
- Secure System Access – Provide the necessary authorizations and credentials to access government systems and infrastructure for the assessment, subject to security protocols.
- Logistical Support – Offer coordination and scheduling assistance for meetings, site visits, and validation sessions as required.

G. LOCATION

The assignment will be conducted remotely and on-site in Malawi, primarily at government data centres, relevant ministries, and agencies where critical digital infrastructure is hosted. The Consultant will be required to undertake field visits to Lilongwe (primary location), Blantyre, Mzuzu and Zomba to conduct assessments, penetration testing, and training sessions.

Virtual engagements may be conducted where feasible; however, on-site presence will be required for critical phases, such as system assessments, penetration testing, and knowledge transfer sessions.

H. KNOWLEDGE TRANSFER

Knowledge transfer is considered an integral part of this assignment and should be reflected in the consultant methodology and technical proposal. Ideally, Government should be able to learn how to replicate / update key element of the assignment, if needed, in future.

I. STAKEHOLDER CONSULTATION

The Consultant is expected to engage 30 MDAs in stakeholder consultation to deliver the assignment, which should be documented, and shared with the Department of e-Government.

J. REQUIRED EXPERIENCE: FIRM & CORE TEAM

The bidder shall demonstrate their capacity, expertise, resources, and reliability to execute the assignment. Among others, they must demonstrate the following eligibility standards:

1. Technical Expertise and Skilled Workforce
   - The Consultant should be well-versed in Network Security & Architecture, Operating System Security, Web and Application Security, Cloud Security, Database Security, Wireless Security, Social Engineering Techniques, Scripting and Automation.
   - The Consultant should have a team that possess certifications such as CCIE Security, CCNP Security, CEH, CEH, CISM, CISSP, CISSP, GWAPT, OSCP, OSWE
   - The Consultant should be proficient in Penetration Testing Tools such as Automated Scanners (Nessus, OpenVAS, Qualys, Burp Suite), Exploitation Frameworks (Metasploit, Cobalt Strike), Network Analysis Tools (Wireshark, Nmap) and Web Security Testing Tools(OWASP ZAP, SQLmap)
   - The Consultant should provide copies of CVs including copies of Professional Certifications / Training Certificates for key staff skills required for the assignment.

2. Experience in Vulnerability Assessment and Penetration Testing (VAPT)
   - Years of experience: The Consultant should have not less than 5 years' relevant experience in VAPT projects, especially working with government agencies, finance, telecom, or enterprise environments.
   - Client References: To demonstrate their experience, the Consultant should be able to provide references from at least three (3) clients where the bidder provided a

similar kind of work in the last five (5) years, who can attest to the quality of their services and ability to meet expectations.

3. Compliance and Security Standards
    - Regulatory Compliance: The Consultant should be familiar with Cybersecurity Standards & Frameworks such as OWASP Top 10, MITRE ATT&CK Framework, GPDR, NIST Cybersecurity Framework, ISO/IEC 27001 and PCI DSS
    - Electronic Transactions and Cyber Security Act, 2016

4. Project Management Capabilities
    - Structured Approach: The Consultant should offer a clear, structured methodology for managing the assignment, including objectives setting, scope definition and risk management plan.
    - Resource and Team Management: The Consultant should assign qualified security experts to the project with clearly defined roles and responsibilities. The Consultant shall maintain effective communication by keeping stakeholders informed through regular meetings and progress reports.
    - Risk Management: The Consultant should have a solid risk assessment and change management in place, prepared to handle security risks, change control process and incident management.

5. Financial Stability and Reputation
    - Financial Health: The Consultant should demonstrate financial stability, ensuring that it can provide long-term services without interruptions due to financial instability.
    - Reputation in the Market: The Consultant should have a strong reputation in the industry as far as VAPT is concerned, with positive feedback from existing clients, and case studies.
    - Incorporation: The Consultant should provide evidence of company registration and tax compliance.

Core Team Composition
The firm shall propose a core team comprising at minimum: a Team Leader, four (4) technical experts, plus any additional support staff necessary to deliver the assignment. All team members must be fluent in English.

The consulting firm must provide a staffing plan with names, roles, and CVs for the core project team as part of the proposal.

Key Positions & Qualifications

Position	Experience	Qualifications
(1) Team Leader (Cybersecurity Expert)	Min. **10 years'** experience in cybersecurity, penetration testing, and risk management. Led **at least 5 similar assignments**, with **at least 3** as a Team Leader or equivalent.	Master's degree in **Cybersecurity, Information Security, Computer Science, IT, or a related field.** Certifications such as **CISSP, CISM, OSCP, or CEH** preferred.
(1) Network Security Specialist	Min. **7 years'** experience in network security, vulnerability assessments, and penetration testing. Experience with at least 2 government or enterprise-scale networks.	Bachelor's or Master's degree in **Computer Science, IT, Cybersecurity, or a related field.** Certifications such as **CCNP Security, CCIE Security, or CISSP** preferred.
(1) Application Security Specialist	Min. **5 years'** experience in secure software development, web application security, and penetration testing. Experience conducting at least 2 **OWASP-based** security testings.	Bachelor's or Master's degree in **Software Engineering, IT Security, or a related field.** Certifications such as **OSWE, CEH, or GWAPT** preferred.
(1) Cybersecurity Training & Awareness Specialist	Min. 5 years' experience in designing and delivering cybersecurity training. Experience conducting at least 2 hands-on workshops and knowledge transfer.	Bachelor's or Master's degree in **Education, Cybersecurity, IT, or a related field.** Certifications such as **CISSP, CISM, or relevant training credentials preferred.**
(1-2) Cybersecurity Analysts / Consultants	Min. 3 years' experience in cybersecurity assessments, penetration testing, and security operations. Experience with government IT environments is an advantage.	Bachelor's degree in Cybersecurity, IT, Computer Science, or a related field. Certifications such as CompTIA Security+, CEH, or equivalent preferred.