Terms of Reference (TOR) for Vulnerability Assessment and Penetration Testing (VAPT) for Kenya Association of Manufacturers (KAM)

1. Introduction

The Kenya Association of Manufacturers (KAM) was established in 1959 as a private sector body and has evolved into a dynamic, vibrant, credible, and respected business membership association that unites industrialists and offers a common voice for businesses.

KAM provides an essential link for cooperation, dialogue, and understanding with the Government by representing the views and concerns of its members to the relevant authorities. In pursuit of its core mandate of policy advocacy, KAM promotes trade and investment; upholds standards; and encourages the formulation, enactment, and administration of sound policies that facilitate a competitive business environment and reduce the cost of doing business.

2. Background

The Kenya Association of Manufacturers (KAM) seeks to enhance its cybersecurity posture by identifying and addressing vulnerabilities within its ICT infrastructure. As part of its commitment to secure operations, KAM is soliciting services from a qualified service provider to conduct a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) across its IT environment. The goal of this exercise is to identify potential vulnerabilities that could be exploited by cyber attackers, assess the effectiveness of existing security measures, and recommend remediation steps.

3. Objectives

The primary objective of the VAPT exercise is to:

- Identify vulnerabilities in KAM's network, systems, and applications.
- Assess the risks associated with the identified vulnerabilities.
- Test the effectiveness of existing security controls.
- Provide actionable recommendations to mitigate identified risks.
- Ensure compliance with cybersecurity best practices and relevant regulations, including data privacy laws.

4. Scope of Work

The scope of the VAPT engagement will include, but is not limited to, the following areas:

4.1 Vulnerability Assessment

- **Internal and External Network Scanning**: Identify vulnerabilities within KAM's internal and external networks, including firewalls, routers, and network infrastructure.
- **Application Security Testing**: Perform vulnerability assessments on KAM's web applications, portals, and any third-party applications integrated into the system.
- **Cloud Infrastructure Security**: Assess vulnerabilities within cloud services used by KAM (if applicable), such as SaaS or PaaS platforms.
- **Operating System & Database Security**: Assess vulnerabilities in operating systems and databases used by KAM.

- **Endpoint Security**: Scan and evaluate security measures implemented on endpoint devices (desktops, laptops, mobile devices).
- **Wireless Network Security**: Assess the security of KAM's wireless network infrastructure.

4.2 Penetration Testing

- **Network Penetration Testing**: Conduct external and internal penetration testing to simulate attacks and identify exploitable vulnerabilities in KAM's network.
- **Web Application Penetration Testing**: Simulate attacks on KAM's web applications to identify flaws such as injection attacks, cross-site scripting (XSS), and session management weaknesses.
- **Social Engineering**: Conduct social engineering tests (e.g., phishing) to assess the organization's vulnerability to human-based attacks.
- **Wireless Network Testing**: Perform penetration testing on KAM's wireless networks to identify weaknesses in encryption, authentication, and access control.
-

5. Deliverables

The selected service provider is expected to deliver the following:

- **Vulnerability Assessment Report**: A detailed report outlining identified vulnerabilities, their associated risks, and recommended remediation steps.
- **Penetration Testing Report**: A comprehensive report on the penetration testing activities, including vulnerabilities exploited, impact assessments, and recommended fixes.
- **Executive Summary**: A high-level overview of the key findings and recommendations suitable for senior management.
- **Remediation Roadmap**: A step-by-step guide to address and remediate identified vulnerabilities, including timelines and resources required.
- **Post-Remediation Validation**: A follow-up test to validate that the vulnerabilities have been successfully remediated.
- **Cyber awareness training**: Conduct cyber awareness training for all staff.

6. Methodology

The service provider should use a combination of automated and manual testing techniques based on recognized standards such as:

- Open Web Application Security Project (OWASP)
- National Institute of Standards and Technology (NIST)
- Information Systems Security Assessment Framework (ISSAF)
- Penetration Testing Execution Standard (PTES)

The assessment should be conducted in a controlled manner to ensure minimal disruption to KAM's operations. The provider must ensure the confidentiality and integrity of the data and systems during testing.

7. Duration of the Assignment

The VAPT exercise should be completed within 6 weeks from the start date, including the assessment, reporting, post-remediation validation and staff training.

8. Required Expertise

The service provider should meet the following qualifications:

- Demonstrable experience conducting VAPT for medium to large organizations.
- Certifications such as Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), or Certified Information Systems Security Professional (CISSP).
- Experience with cybersecurity standards and frameworks, including OWASP, NIST, and ISO 27001.
- Proven track record in delivering actionable security recommendations.

9. Confidentiality and Data Protection

The service provider will be required to sign a Non-Disclosure Agreement (NDA) and comply with all applicable data protection laws, including the Data Protection Act 2019 (Kenya), to ensure the confidentiality of KAM's information.

10. Submission of Proposals

Interested service providers should submit their technical and financial proposals detailing the following:

- Methodology and approach to be used for VAPT.
- Detailed work plan and timeline.
- Relevant experience and case studies.
- Team composition and qualifications.
- Financial quotation (cost breakdown).
- Statutory documents:
    - Company registration certificate
    - Company CR12
    - Company PIN
    - A valid company TCC

Submission Deadline: The proposals are to be submitted to the attention of the Procurement Manager, KAM House 5th floor. 15 Mwanzi Road, Opp Westgate Mall by 1st August 2025, at 4.00 p.m. Late submissions will not be opened.

Please Label the Envelope "V**ulnerability Assessment and Penetration Testing (VAPT)**"

11. Evaluation Criteria

- A two-stage procedure will be utilized in evaluating the proposals, with an evaluation of the technical component being completed before any price component. Scores will be awarded for the technical proposal with:
    - Understanding of the scope and objectives.
    - Approach and methodology.
    - Qualifications and experience of the team.

- The price component proposal will be opened only for those firms/ institutions whose technical component meets the requirements for the assignment, as indicated by a score of more than 70%.

12. Payment terms (provisions)

Kenya Association of Manufactures policy is to pay for contractual services based on the performance of contractual services rendered. For this task, KAM intends to make all payments upon completion of the assignment.

Please note only successful candidates will be contacted