KCMC UNIVERSITY

P. O. Box 2240, MOSHI,
Tanzania.
Email: info@kcmcu.ac.tz

Telephone +255-027-2753616.
Fax: +255-027-2751351.
Web site: http://www.kcmcu.ac.tz

ICT DIRECTORATE

TERMS OF REFERENCE (ToR)

FOR CONDUCTING A COMPREHENSIVE VULNERABILITY AND SECURITY ASSESSMENT OF ICT INFRASTRUCTURE, SYSTEMS, APPLICATIONS AND RELATED DIGITAL ASSETS

Reference No.	KCMC/ICT/TOR/2026/28726
Issuing Office	ICT Directorate, KCMC University
Assignment Title	Vulnerability and Security Assessment of Institutional ICT Infrastructure
Type of Engagement	Consultancy / Professional Service (Firm)
Duty Station	KCMC Main Campus, Moshi, Tanzania (on-site and remote as required)
Estimated Duration	[To be confirmed] weeks from contract signing

1. Background and Context

KCMC University operates a growing portfolio of ICT infrastructure, systems, applications, and digital assets that support teaching, research, clinical training, administration, and student welfare functions across the institution. The ICT Directorate provides enabling infrastructure across all five Key Results Areas (KRAs) of the institution's Five-Year Rolling Strategic Plan (FYRSP 2025/26–2029/30), and bears responsibility, including at Senate level, for the security, integrity, and reliability of these systems.

In alignment with the implementation of the ICT Annual Action Plan for FY 2025/2026, the ICT Directorate seeks to engage a qualified and experienced firm to conduct a comprehensive Vulnerability and Security Assessment of the institution's ICT infrastructure, systems, applications, and related digital assets. This engagement is a proactive measure to identify existing security weaknesses, evaluate the institution's exposure to cyber threats, and obtain actionable recommendations for strengthening the overall cybersecurity posture of the institution.

2. Objectives of the Assignment

The overall objective of this assignment is to conduct a comprehensive vulnerability and security assessment covering both the technical and operational aspects of information security at KCMC. Specifically, the assignment shall:

1. Identify existing security weaknesses and vulnerabilities across the institution's network, systems, applications, and digital assets.
2. Evaluate the institution's exposure to prevailing and emerging cyber threats.
3. Assess the effectiveness of existing technical and operational security controls.
4. Determine the severity and potential business impact of identified vulnerabilities and risks.
5. Recommend practical, prioritized, and cost-effective mitigation measures to strengthen the institution's overall cybersecurity posture.
6. Provide KCMC University Management and the ICT Directorate with a clear, evidence-based report to guide remediation planning and future security investment.

3. Scope of Work

The Consultant/Firm shall carry out a comprehensive assessment covering, but not limited to, the following areas:

3.1 Network Vulnerability Assessment

Assessment of internal and external network infrastructure, including identification of exposed services, misconfigurations, and exploitable vulnerabilities.

3.2 Web Application Security Assessment

Security testing of institutional web-based systems and portals, including but not limited to authentication mechanisms, session management, input validation, and common web application vulnerabilities (e.g., OWASP Top 10).

3.3 Server and Endpoint Security Review

Review of server and endpoint operating systems, hardening status, patch levels, configurations, and access controls.

3.4 Network Device Configuration Review

Review firewall, router, and switch configurations, where applicable, to identify misconfigurations and deviations from security best practices.

3.5 Wireless Network Security Assessment

Assessment of wireless network infrastructure, encryption standards, authentication mechanisms, and segmentation controls.

3.6 Database Security Assessment

Assessment of database platforms supporting critical institutional systems, including access controls, configuration hardening, and data protection measures.

3.7 User Access and Privilege Review

Review of user account management practices, access provisioning and de-provisioning processes, and privilege assignment across critical systems.

3.8 Risk Identification and Remediation Guidance

Identification and classification of risks and vulnerabilities by severity level, together with recommended, prioritized remediation actions for each finding.

3.9 Reporting

Preparation and submission of a detailed technical report and a concise executive summary report, each with prioritized, actionable recommendations.

The scope outlined above represents the minimum expected coverage. The engaged firm may, in its technical proposal, recommend additional assessment areas relevant to a comprehensive institutional security posture review, for consideration by the ICT Directorate.

4. Approach and Methodology

The engaged firm is expected to propose a methodology aligned with recognized industry standards and frameworks (such as OWASP, NIST, ISO/IEC 27001, or PTES), and shall, as a minimum, address the following:

- Planning and scoping, including agreement of rules of engagement with the ICT Directorate.
- Information gathering, reconnaissance, and asset/system inventory validation.
- Automated vulnerability scanning complemented by manual verification and testing.
- Risk rating of findings using a recognized severity classification scheme (e.g., Critical, High, Medium, Low).
- Validation of findings with relevant ICT Directorate personnel prior to final reporting.
- Safe testing practices that avoid disruption to live institutional systems and services, with any potentially disruptive tests conducted under prior written agreement and appropriate scheduling.

5. Deliverables

The Consultant/Firm shall submit the following deliverables:

7. Inception report outlining the confirmed scope, methodology, rules of engagement, and work plan/timeline.
8. Detailed technical report presenting all findings, evidence, risk/severity ratings, affected assets, and recommended remediation actions.
9. Executive summary report presenting a non-technical overview of the institution's security posture and prioritized recommendations, suitable for presentation to Management and Senate.
10. A remediation roadmap/action plan indicating recommended timelines and responsible parties for addressing identified findings.
11. A closeout presentation to the ICT Directorate (and Management, as required) summarizing key findings and recommendations.
12. Where retesting is included in the proposal, a verification report confirming remediation of previously identified critical and high-severity findings.

6. Duration and Timeline

The assignment is expected to be completed within a period to be proposed by the bidding firm and agreed with the ICT Directorate, inclusive of planning, on-site/remote assessment, analysis, and reporting phases. Prospective firms shall submit a detailed work plan with milestones as part of their technical proposal.

7. Qualification Requirements for the Firm

Interested firms shall demonstrate the following minimum qualifications:

- Proven track record and demonstrable experience in conducting vulnerability assessments and/or penetration testing for institutional, higher education, health-sector, or similarly complex ICT environments.
- Relevant professional certifications held by assigned personnel (e.g., CEH, OSCP, CISSP, CISM, CompTIA Security+, or equivalent).
- Registration/incorporation as a legally recognized business entity, with a valid business/operating licence and Tax Identification Number (TIN).
- Evidence of similar assignments completed for comparable institutions, including reference contacts.
- Adequate technical capacity, tools, and methodology to execute the full scope of work described in this ToR.
- Willingness to sign a confidentiality/non-disclosure agreement and to comply with KCMC University's data protection and information security policies.

8. Confidentiality and Data Protection

All information, data, findings, and reports arising from this assignment are strictly confidential and remain the property of KCMC. The engaged firm and its personnel shall sign a Non-Disclosure Agreement (NDA) before commencement of work and shall handle all institutional data, credentials, and findings in accordance with applicable data protection requirements. Testing shall be conducted only within the agreed rules of engagement, and no findings, data, or institutional information shall be disclosed to any third party without prior written authorization from KCMC.

9. Management and Reporting Arrangements

The assignment shall be coordinated by the ICT Directorate, which shall serve as the primary point of contact for the engaged firm. All deliverables shall be submitted to, and reviewed by, the Director of ICT (or a designated officer), with findings ultimately reported for Management and, where applicable, Senate-level consideration.

10. Evaluation Criteria

Proposals received shall be evaluated based on, but not limited to, the following criteria:

- Technical competence, proposed methodology, and understanding of the assignment.
- Qualifications and certifications of proposed personnel.
- Relevant prior experience and references.
- Proposed work plan and timeline.
- Financial proposal and value for money.

11. Submission Requirements

Interested and qualified firms are invited to submit both technical and financial proposals, together with company profile, relevant certificates, and references, to the address/contact indicated in the accompanying request/procurement notice, on or before the specified closing date.

Annex: Attachments

- Form No. 2 as referenced in the covering request letter.

Prepared by:
Gabriel J Msuka

Director of ICT
KCMC University