TERMS OF REFERENCE

Provision of System Audit, Vulnerability Assessment, and Penetration Testing Services.

1.0 INTRODUCTION

German Sparkassenstiftung Eastern Africa (DSIK) is a German-based NGO with global headquarters in Bonn, Germany, targeting poverty reduction through sustainable financial inclusion. To reach its goal, DSIK partners with local organizations to jointly conduct project activities. The main interventions are targeted towards professionalizing and digitalizing the microfinance and SACCOS sectors, increasing financial literacy, capacity development, and institutional strengthening.

In Tanzania, DSIK is providing advisory services to the Savings and Credit Cooperative Union League of Tanzania (SCCULT). Project activities in Eastern Africa are not limited to Tanzania, but also include Burundi, Kenya, Rwanda, and Uganda. In Tanzania, DSIK is a registered International Non-Governmental Organization under The Non-Governmental Organization Act, 2002 made under Section 11 (1) and 17 (2) of Act No. 24 in 2002 with Registration No. I-NGO/R1/005.

Within this initiative, DSIK is set to collaborate closely with SCCULT, the umbrella organization for SACCOS in Tanzania mainland. Established in 1992 under the Cooperative Act 15, SCCULT is dedicated to empowering and advancing SACCOS through advocacy, financial assistance, and technical support. SCCULT (1992) Ltd is licensed under the Microfinance Act of 2018, holding license number MSP3-TCDC/2021/00374 issued in 2021.

2.0 PROJECT BACKGROUND

In 2022, the Savings and Credit Cooperative Union League of Tanzania (SCCULT) set out to design, develop, and implement a Shared Core SACCOS System (CSS). This initiative was in response to the low adoption rate of information and communication technologies (ICT) within the SACCOS sector. According to the 2022 SACCOS annual report[1], only 10.13% of SACCOS were utilizing ICT systems. The slow adoption was primarily attributed to the lack of reliable system vendors and the high costs associated with available systems, making them unaffordable to SACCOS.

Within this initiative, SCCULT aimed to introduce a Core SACCOS System (CSS) that would serve as a shared service for all SACCOS. As the umbrella organization for SACCOS, SCCULT was acutely aware of the digitalization issues faced in the cooperative sector. The CSS was envisioned as a solution to these challenges, facilitating a collaborative resource pool accessible to all SCCULT members. This approach was therefore intended to minimize resource expenditure by lowering fees, ensuring seamless execution of essential tasks, and promoting optimal compliance, efficiency, and cost-effectiveness within the sector.

Through a collaborative partnership involving SCCULT as the business owner, UBX as the system developers, Umoja Switch as a digital payment service provider, and DSIK as project advisors, the

[1] Tanzania Cooperative Development Commission (2023) *The Savings and Credit Cooperative Societies (SACCOS) Annual Report for 2022, The Annual Report on Operations, Performance and Supervision of SACCOS in Tanzania, Second Edition, 2023,* https://www.ushirika.go.tz/uploads/THE_SAVINGS_AND_CREDIT_COOPERATIVE_SOCIETIES_(SACCOS)_ANNUAL_REPORT_FOR_2022.pdf [03.03.2024]

successful development and initial deployment of the Shared Core SACCOS System have been achieved. Currently, the project is progressing with the onboarding of SACCOS.

3. 0 OBJECTIVES

The objective of this assignment is to identify and evaluate potential security vulnerabilities, assess the system's performance, and ensure compliance with industry regulations and best practices through a thorough **System Audit, Vulnerability Assessment, and Penetration Testing for the Shared Core SACCOS System.**

The purpose of this engagement is to guarantee the reliability, integrity, security and regulatory compliance of the developed Core SACCOS System.

4.0 SCOPE OF WORK

This assignment entails conducting a comprehensive system audit, vulnerability assessment, and penetration testing for the developed Shared Core SACCOS System.

The scope of this assignment will encompass the areas below and is expected to deliver the required outputs within **fifteen (15) working days:**

4.1 System Audit

The system audit shall review the system's processes, controls, and compliance with relevant standards and regulations to ensure operational integrity and efficiency. This shall include:

(i) **Access Controls**: Review the access control mechanisms to ensure they effectively protect sensitive information against unauthorized access, data breaches, and other security threats.
(ii) **Internal Controls and Security Procedures**: Evaluate overall security architecture, controls, and procedures, including network security, application security, data security, endpoint security, audit trails, system monitoring, and maintenance, as well as controls over program and system changes to ensure they are effective in mitigating risks and ensuring proper system operation.
(iii) **Evaluating System Performance**: Ensuring the system operates efficiently and meets performance requirements, including speed, reliability, resource usage, and ability to handle expected workloads.
(iv) **Verifying Compliance**: Checking adherence to relevant laws, regulations, and internal policies to ensure legal and regulatory compliance, such as Data Protection laws, Financial Regulations, and Industry Standards.
(v) **Identifying Risks**: Detecting potential risks and vulnerabilities in the system and assessing their impact on business operations.
(vi) **Data Integrity**: Ensuring the accuracy, consistency, and reliability of data within the system by evaluating data protection measures such as encryption, data masking, and anonymization and ensuring compliance with data privacy regulations.
(vii) **BCM and Disaster Recovery:** Evaluate the incident response plan, including detection, response, and system's ability to recover from unexpected shutdowns and its capability to recover from disasters resulting in data loss.

(viii) **Accurate Financial Reporting**: Verifying that financial data and transactions are accurately recorded and reported in compliance with financial regulations and accounting standards.
(ix) **Recommending Improvements**: Providing suggestions for enhancing system performance, security, and overall effectiveness based on audit findings.
(x) Prepare reports in outlined format.

4.2 Vulnerability Assessment

The vulnerability assessment will identify potential security weaknesses and risks within the system that could be exploited. The consultant shall therefore provide vulnerability assessment services including but not limited to the following:

(i) Conduct a physical security assessment of the CSS facilities and assets.
(ii) Conduct external and internal vulnerability scans to identify any security vulnerability that may exist in CSS software, hardware assets, and integration points.
(iii) Assess current network security measures to identify any vulnerability that may exist within the CSS architecture.
(iv) Conduct OWASP web application security assessment.
(v) Ensure that security issues that pose an imminent threat are reported as they are being identified.
(vi) Assess the potential impact and likelihood of each identified vulnerability, prioritizing them based on their risk level.
(vii) Provide detailed recommendations for mitigating identified vulnerabilities, including technical fixes and policy changes.
(viii) Prepare a report in outlined format.

4.3 Penetration Testing

Finally, the penetration test will simulate cyber-attacks to test the system's defenses and uncover any vulnerabilities that need to be addressed. The consultant shall therefore provide the following quality penetration testing services:

(i) Application/website penetration testing services. These shall include:
    a) Authentication process testing
    b) Development of test datasets and harnesses
    c) Testing systems for user session management to see if unauthorized access can be permitted including but not limited to:
        - Input validation of login fields
        - Cookie security
        - Lockout testing
    d) User session integrity testing
    e) Encryption usage testing (e.g., applications' use of encryption, sensitive data exposure)
    f) Testing of the application functionality including but not limited to:
        - Input validation (e.g., bad, or over-long characters, URLs)
        - Transaction testing (e.g., ensuring desired application performance)

g) Injection

(ii) Network penetration testing services. These shall include but are not limited to:
   a) Identify targets and map attack vectors (i.e., threat modelling)
   b) Spoofing
   c) Brute force attacks
   d) Network sniffing
   e) Trojan attacks
   f) Denial of Service ("DDoS") testing

(iii) Social engineering testing services

(iv) Other penetration testing services

(v) Prepare a report in outlined format.

Note: The consultant shall provide system testing services following appropriate industry-wide, highly recognized methodologies and standards such as:

- National Institute of Standards and Technology ("NIST") SP 800-42
- Open-Source Security Testing Methodology Manual ("OSSTMM")
- Penetration Testing Execution Standard ("PTES")
- Open Web Application Security Project ("OWASP")

The consultant must ensure proper cleanup after completing system testing, making sure that the CSS environment is not impacted. Cleanup activities shall include, but are not limited to, the following:

(i) Update and/or removal of test accounts added or modified during testing

(ii) Update and/or removal of database entries added or modified during testing

(iii) Restoring security controls that have been altered for testing

(iv) Uninstalling any test tools as applicable

(v) Provide guidance/necessary information on how to verify that the system environment has been restored

(vi) Provide confirmation that the system environment has been cleaned and restored

5.0 KEY DELIVERABLES

The expected deliverables in this assignment are:

a) **Three Full Reports** – System Audit Report, Vulnerability Assessment Report and Penetration Testing Report. The full reports shall each include all assessment raw data, summary data and recommendations.
b) **Executive Report** of each of the full reports. The executive report shall include summary data and recommendations.
c) **Retesting Report** – includes all identified/exploitable vulnerabilities that require immediate remediation, this to be provided after remediation and retesting.

5.1 Reporting Guidelines

5.1.1 Full Report Outline

Each of the full reports shall contain at a minimum:

(i) Executive Summary. A brief high-level summary of the assessment/scope and major findings
(ii) Statement of Scope. A detailed definition of the scope of the system and network tested / assessed. This section should outline the boundaries of the assessment, including which components of the system and network were included in the testing. Additionally, identify the critical processes and explain the rationale for including them as targets in the test.
(iii) Statement of Methodology. Details on the methodologies used to complete the testing. The methodologies and standards used should be explicitly stated as well.
(iv) Statement of Limitations. Document any restrictions imposed on testing, including designated testing hours, bandwidth limitations, special testing requirements, and any other relevant constraints.
(v) Testing Narrative. Provide details as to the testing methodology and how testing progressed, document any issues encountered during testing.
(vi) Segmentation Test Results - summarize the testing performed to validate segmentation controls
(vii) Findings
- Tools Used
- Whether/how the findings may be exploited
  Risk ranking/severity of each vulnerability
- Targets affected
- Description of finding
- References (if available)

5.1.2 Executive Report Outline

The executive report shall contain at minimum:

(i) Executive Summary. A brief high-level summary of the assessment/test scope and major findings
(ii) Statement of Scope. A definition of the scope of the systems and network tested. An identification of critical system components and processes as well as an explanation of why they are included in the test as targets

(iii) Findings

- Whether/how the findings may be exploited
- Risk ranking/severity of each vulnerability
- Targets affected
- Description of findings

5.1.3 Retesting Report Outline

If any findings require remediation and retesting, a follow-up test report may be provided. All remediation efforts should be completed and retested within a reasonable time after the original test/assessment report is issued. The follow-up report should address all identified and exploitable vulnerabilities that require immediate remediation.

When retesting is necessary, the report shall contain at least:

(i) Executive Summary
(ii) Date of Original Test
(iii) Date of Retest
(iv) Original Findings
(v) Results of Retest

6. QUALIFICATION AND EXPERIENCE OF THE CONSULTANT(S)

The applicant should have relevant qualifications and working experience, particularly:

(i) At least a Bachelor's Degree in Cybersecurity, Information and Communication Technologies (ICT), Information Technology (IT), Digital Finance, or a related field.
(ii) Specialized cybersecurity certifications such as Computer Hacking Forensics Investigator (CHFI), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified Ethical Hacker (CEH), Pen Test or related field.
(iii) At least 7 years of working experience in Cybersecurity and at least 10 years of experience in ICT or Digital Finance.
(iv) A comprehensive knowledge on financial and cybersecurity regulations, policy updates, and circulars applicable to the financial sector in Tanzania.
(v) Must be a professional registered with the Tanzania Communications Regulatory Authority (TCRA) to provide system audit and vulnerability assessment services.
(vi) Proven working experience in conducting system audits, vulnerability assessments and penetration testing.
(vii) Experience in communicating effectively with a diverse team of partners.
(viii) Certified in Risk and Information Systems Control (CRISC), and Certified Information Systems Security Professional (CISSP), will be an added advantage.
(ix) Proficient in producing concise reports.

An eligible consultant may either be an individual or a firm.

7. MODE OF APPLICATION/BIDDING REQUIREMENTS:

Interested consultants should submit both Technical and Financial Proposals for this assignment. A technical proposal detailing their approach to the assignment, methodology, and work plan. Financial Proposals should provide, among other things, a breakdown of costs, and the bidders should be **VAT registered** (if it is a firm) and must be able to provide **Electronic Fiscal Device Receipts (EFDs)**. The proposals should be accompanied by the Company Profile (for firms), CVs of the responsible team, Address (PO Box), Phone Number, Email Address, Physical Address, and list of both the previous and current Corporate Customers.

The proposals should be submitted to the following e-mail by **5th September 2024** at 17:00 (EAT): Office.Tanzania@dsik.org

Please be informed that candidates who will not hear responses by **12th September 2024** should consider themselves unsuccessful.

For any enquiry you may contact: Ms. Kalunde Kapaliswa via Tel: +255 766 0202 84 or E-Mail: Kalunde.Kapaliswa@dsik.org