SHIRIKA DEPOSIT TAKING SACCO SOCIETY LTD

TERMS OF REFERENCE (TOR)

FOR

THE CONSULTING SERVICES FOR SHIRIKA DEPOSIT TAKING (SDT) SACCO LTD SYSTEM AUDIT OF THE CORE BANKING SYSTEM (DYNAMIC 365 BUSINESS CENTRAL V24) AND ICT DEPARTMENT CAPACITY ASSESSMENT

Client:

Shirika DTS Society Limited

P.O Box 43429-00100,

Nairobi

Email : info@shirikasacco.co.ke

2025

BACKGROUND

Shirika DT Sacco was registered on 24th April 1969 under the Co-operative Societies Act of the Laws of Kenya. The Society is regulated by SASRA and has a membership of over 10,000.

The Sacco is using Dynamic 365 BC as Core Banking System which is hosted on premise. The System upgrade from Navision 2016 to Dynamic 365 was carried out in June 2024.There are other applications within the Core Banking System that are integrated e.g. Mobile banking, ATM and member portal. The information system is valued as part of Shirika DT Sacco internal control systems. The system does not merely record business transactions, but drives the key business processes in line with the policies in place. The ICT industry is very dynamics with new innovations adoption that drives operation. Cyber security remains a critical concern for many organizations especially those offering financial services.

Objective(s) of the Assignment.

Shirika DT Sacco believes that information systems and process reengineering audit is a part of the overall audit process, to ensure control maximization and risk mitigation. It seeks an independent and objective assurance to determine whether the information systems, related resources and the environment adequately safeguard assets, maintain data and system integrity; provide relevant and reliable information; achieve organizational/information system goals and consume resources efficiently and have internal controls that provide reasonable assurance that operational and control objectives will be met, undesired events will be prevented, detected & rectified in a timely manner. Additionally, that the information system could be reengineered to improve process timelines.

Scope of assignment and Specific tasks

IS and process reengineering auditor is required to provide assurance on technology infrastructure, application and associated internal control framework by assessing the CORE Business System 365 functionality, efficiency, accuracy and security through risk assessment, internal control evaluation and detailed testing of associated data. The

consultant will be expected to provide areas of improvement to improve the processes.

Specific task includes

The IS and process reengineering Auditor is expected to adopt a risk-based approach to making an audit plan. The IS auditor is required to refer towards framework and standards on information system developed by ISACA. **The major elements of audit will be classified as follows**:

1. **Network Security and System Controls Review:**
   - **Assessment of Current Network Security:** Review the existing network security controls to identify strengths, weaknesses, and areas for improvement. Recommendations for enhancing the security posture will be provided.
   - **Assessment of User Activity Controls:** Evaluate the adequacy of controls and procedures in identifying, tracking, and managing user system activities to prevent unauthorized access and maintain accountability.
   - **System Configuration and Change Management:** Review configuration management processes, including changes in system architecture, to ensure proper security controls and minimize vulnerabilities.
   - **Application and WAN Security Review:** Evaluate security measures for applications and Wide Area Network (WAN), ensuring they meet security standards and protect against threats like unauthorized access and data breaches.
2. **Cyber Risk Assessment and Vulnerability Management:**
   - **Cyber Risk Assessment:** Evaluate the Sacco's digital infrastructure for resilience against cyber threats. Identify vulnerabilities, monitor potential risks, and assess compliance with data privacy regulations. Propose methods to manage these risks effectively.
   - **Penetration Testing & Vulnerability Assessment:** Conduct both internal and external penetration testing to simulate attacks and identify vulnerabilities in the system. This includes testing password strength, email/web security, firewall configurations, server/database security, and VPN security.
   - **Virtual Environment Security Testing:** Test virtual environments for weaknesses and potential vulnerabilities that could expose the system to cyber threats.
3. **System and Application Software Review:**
   - **Application Software Review:** Assess the security, access control, exception handling, business process flows, and report validation (both financial and operational) of financial and operational applications to ensure they meet organizational and regulatory needs.
   - **Report Validation:** Audit reports produced by the system to verify that calculations, data integrity, and the functionality of reports meet industry best practices.
4. **Data Security and Integrity:**
   - **Data Integrity Review:** Review the database design, structure, and controls to

ensure data is accurate, consistent, and protected against unauthorized alterations. This also includes testing live data to evaluate the system's performance and identifying potential weaknesses.

5. **Business Continuity and Disaster Recovery:**
   - **Business Continuity Review:** Ensure fault tolerance and redundancy in hardware, robust backup procedures, and a documented disaster recovery plan. Evaluate the effectiveness of the recovery process and its compliance with the business continuity plan.
   - **Disaster Recovery/Business Continuity Plan Effectiveness:** Assess the testing and implementation of disaster recovery procedures and the overall reliability of the business continuity strategy.
6. **Security of Integration and Interfaces:**
   - **Integration and System Interfaces Review:** Evaluate the integration of the system with existing platforms (e.g., MPESA, ATM, Mobile Banking Systems, databases) to ensure security and compliance with integration requirements.
7. **Website Security and Social Engineering:**
   - **Website Penetration Testing:** Perform penetration testing on the website to identify vulnerabilities and assess its resilience against cyber threats.
   - **Social Engineering Assessment:** Conduct simulated social engineering attacks to assess the security awareness of users and the effectiveness of training programs to protect against such threats.
8. **Domain Controller and Configuration Review:**
   - **Domain Controller Configuration Testing:** Assess the configurations of domain controllers to ensure they are securely set up and adequately protect the network from unauthorized access or manipulation.
9. **Process Improvement and Service Delivery:**
   - **Process Improvement:** Identify opportunities to improve security processes, enhance service delivery, and streamline procedures for better efficiency and risk management.
10. **ICT Department Capacity Assessment:**
   - **ICT Department Capability Evaluation:** Assess the overall capacity and competency of the ICT department to handle current and future demands. This includes evaluating the skill levels of IT personnel, resource allocation, technology infrastructure, and their ability to respond to emerging threats.
   - **Training and Knowledge Gaps:** Identify any training gaps in the ICT team, ensuring that they are equipped with the necessary skills to manage new technologies and emerging security risks effectively.
   - **Staffing and Resource Management:** Review staffing levels and workload distribution within the ICT department to ensure adequate support for security functions, incident response, and day-to-day operations.
   - **Technology and Tools Assessment:** Evaluate whether the ICT department has the necessary tools and technologies in place to effectively monitor, manage, and secure the digital infrastructure. This includes reviewing the current software solutions, security technologies, and monitoring systems in use.

Additionally, the IS Auditor must analyze business process risks and controls based on an understanding of planned or implemented controls and identified control gaps. The IS auditor is required to review role of Internal audit in relation to IS audit. This may involve evaluating audit plans and reporting to audit committee and senior management on controls, specific resources required for performing IS audit function.

Experience and qualification

The organization seeks services must be qualified IS auditor and must meet the following.

a) **Core business and years in business:** The firm shall be registered/incorporated as a consulting firm in the field of Audit with specific expertise in system audit for SACCOs or similar operating environment for a period of at least eight (8) years.
b) **Experience:** The firm shall demonstrate as having successfully executed and completed at least two (2) assignments similar in nature both in scope and complexity in a similar operating environment. Details of the assignments (Name and address of the client, scope, value, and period) should be provided and submitted in the submitted proposal)
c) **Technical and managerial capability of the firm:** The firm shall demonstrate as having the requisite technical capacity including relevant equipment, tools, software, etc. and managerial capacity to undertake the assignment in the submitted company profile(s**).**

Experience of Key Technical personnel

Team Leader

Must have a degree in Master of Science in information Technology (ICT and certification on ICT /audit professional body). Experience having performed similar task at least 2 relevant similar assignments in the last 5 Years (with Process reengineering process & past experience with Dynamic 365 BC for Sacco's (preferably Deposit taking SACCO development)

Key expert 1: Software engineer

Master degree on software development or relevant field. Demonstrate have conducted similar task in the last three years in busy ICT environment preferably financial institution

Key expert 2: Database expert

Must have Bachelor degree in ICT, computer science, computer engineering, statistics demonstrate have conducted similar task in the last three years in busy ICT environment

preferably Financial institution

Certification in business intelligence or development for at least 5 years advanced excel, SQL, SPSS and Experience in developing, SACCO software and data base

Deliverables and timelines for submission

The expected deliverables and timelines for submission of deliverables are in the following table

Table 1: Expected Deliverables

S/No.	Deliverables/Task	Timeline of submission after contract commencement (Months)
1.	Inception Report and detailed Work plan for the assignment	7th Day
2.	Detailed preliminary penetration test report detailing institutional ICT environment of the society (Security, users, functionality of each modules, API integrations, networking and ,key risk identified and mitigation measure	21st days
3.	Comprehensive reports on above	35th day
4.	Final repot …… containing detailed observations on aforementioned areas as well as suggested areas during preliminary meetings with the management. In addition, a detailed roadmap/ recommendations for improvements in risk areas identified.	45th Day
	Total	**45 days**

Duration of the Assignment

This assignment shall be executed and completed within a period of 45 days after contract commencement date. It will be implemented in SDT SACCO ltd premises /non-live environment

6.0 Payment schedule

The proposed payment schedules based on satisfactory performance of the contract which will be negotiated with the successful consultant will be as presented in Table 2.

Table 2: Payment Schedule

S/No.	Report	Payment % of contract amount
1	Submission and acceptance of inception report and work plan	**40%**
2	Submission of Detailed preliminary penetration test and mitigation measure	**30%**
3	Submissions of comprehensive 1st draft report	
6	Submission and acceptance of Final comprehensive report incorporating all key deliverables above and acceptable to the client	**30%**

Management and accountability of the assignment

The consulting services assignment will be conducted with SDT SACCO as the client, with the CEO shall oversee the overall quality control and coordinate various aspects of the assignment. The CEO will share updates on the consultancy's progress and activities with the board on the progress of the activities.

The society CEO of the client will manage the day-to-day coordination of the consultancy, while the Consultant will appoint a counterpart. These two individuals will serve as the primary points of contact for coordinating logistics and administrative details for events such as field missions for data collection, as well as consultative and dissemination workshops. During execution of the assignment, the consultant will work closely with the HODs or any other officer appointed by CEO under these contractual obligations.

11. Obligations of the Client

The SDT Ltd will make available the following resources to facilitate the work of the Consulting firm:

1. All existing society policies where applicable
2. CBS 365 user Manual
3. User right where applicable – on request and in writing
4. All interface API
5. In some cases, the client may provide office space and other facilities.

12. Obligations of the Consultant

i) The Consultant assumes responsibility for the costs of transportation, accommodation, insurance, airtime, and any other related expenditures.
ii) The Consultant is expected to undertake activities that ensure the outputs are consistent with professional and legal requirements.
iii) Furthermore, the data must be generated through a consultative process that guarantees authenticity and ownership will be responsible for such as execution of the assignment in a professional and timely manner, provision of all the necessary resources to carry out the services.

13. Propriety rights of Client in report and records

All the data and information collected or received for the purposes of this assignments will be kept strictly confidential and will be used exclusively to execute the terms of reference. All the intellectual property rights stemming from the execution of the terms of reference belong to SDT Ltd. The content of the written materials that are obtained and utilized during this task will not be shown to third parties without the written consent of the board.

MANDATORY REQUIREMENTS
The following will form part of mandatory requirement for basis of evaluation of technical proposal

i. Current Audited account
ii. Valid Tax certificate
iii. Profile of the Firm including directors
iv. Registration certificate

Interested firms that meet the requirements should submit technical detailing methodology and work plan and financial proposals in a sealed envelope **MARKED S/AUDIT/1/2025** to the address below on or before close of business on Friday 4th Jul, 2025 at 4:00 pm to:

The Chief Executive Officer,
Shirika DT Sacco Society Limited,
P.O. BOX 43429 – 00100,
NAIROBI

The Sacco reserves the right to reject any proposal without giving

reasons