UNITED REPUBLIC OF TANZANIA

MINISTRY OF AGRICULTURE

TANZANIA COOPERATIVE DEVELOPMENT COMMISSION

GUIDELINES ON CYBERSECURITY AND RESILIENCE OF SACCOS IN TANZANIA

Office of the Registrar of Cooperative Societies,
Mtendeni Road,
S.L.P 201,
DODOMA.

Website: www.ushirika.go.tz
Email: ushirika@ushirika.go.tz

Issue Date: October 31, 2024

EXECUTIVE SUMMARY

The "Guidelines on Cybersecurity and Resilience of SACCOS in Tanzania" aim to establish a robust framework for enhancing the cybersecurity posture and resilience of Savings and Credit Cooperative Societies (SACCOS). With the increasing adoption of digital technologies in the financial sector, SACCOS face growing risks from cyber threats that can compromise member data, financial assets, and overall operational continuity.

Purpose

The guidelines provide a structured approach to:

a) Safeguard member data and financial information.
b) Ensure operational continuity and resilience against cyber disruptions.
c) Promote trust and confidence in SACCOS' digital systems.
d) Align SACCOS with national and international cybersecurity standards and practices.

Scope

These guidelines apply to all SACCOS operating in Tanzania, including:

a) Small, medium, and large SACCOS.
b) SACCOS with digital payment platforms or integrated financial systems.
c) Third-party service providers working with SACCOS.
d) Outline measures, procedures and other regulatory framework that SACCOS licensed and regulated by the TCDC should comply.
e) Enhance their cyber posture and resilience.
f) Create a common approach for addressing cyber risk within the SACCOS system.
g) Achieve minimum and acceptable levels of cyber resilience.
h) Ensure that systemic cyber risk is properly managed within the SACCOS system.

Key Provisions

1. Governance and Oversight:
   - Establishing cybersecurity governance frameworks, including policies and accountability structures.
   - Designating cybersecurity officers or teams to oversee and manage risks.
2. Risk Management:
   - Conducting regular cybersecurity risk assessments.

- Identifying critical assets and implementing measures to protect them from threats.

3. Access Control and Data Security:
   - Implementing secure authentication methods.
   - Protecting sensitive member data through encryption and access restrictions.
4. Incident Response and Recovery:
   - Developing and testing incident response plans to manage cyber events.
   - Ensuring prompt recovery of systems to minimize disruptions.
5. Capacity Building and Awareness:
   - Training employees and stakeholders on cybersecurity best practices.
   - Promoting awareness campaigns for members about safe digital behavior.
6. Third-Party Risk Management:
   - Assessing and monitoring the cybersecurity practices of vendors and service providers.
   - Incorporating cybersecurity requirements in contracts.
7. Regulatory Compliance and Reporting:
   - Adhering to applicable cybersecurity laws and standards in Tanzania.
   - Reporting significant cyber incidents to relevant authorities.

Benefits of Implementation

a) Enhanced protection of member data and financial resources.
b) Reduced risk of operational disruptions due to cyber incidents.
c) Increased trust in SACCOS' digital systems, fostering member confidence.
d) Alignment with Tanzania's digital financial inclusion goals.

The guidelines underscore the need for SACCOS to adopt a proactive and resilient approach to cybersecurity. By implementing these measures, SACCOS can mitigate cyber risks, ensure continuity of services, and support the growth of a secure and inclusive financial ecosystem in Tanzania.

Dr. Benson O. Ndiege
THE REGISTRAR OF COOPERATIVE SOCIETIES

Contents

1. AUTHORITY, PURPOSE AND SCOPE 6

1.1 Authority 6

1.2 Applicability 6

1.3 Scope of Authority 6

2. INTRODUCTION 7

3. DEFINITION OF TERMINOLOGY 9

4. CYBER RISK MANAGEMENT AND OVERSIGHT 13

4.1 GOVERNANCE 13

4.1.1. Oversight 13

4.1.2. Cyber-Resilience Strategy 13

4.1.3. Cyber-Resilience Framework 14

4.1.4. Board and Senior Management Responsibilities 15

5. CYBER-SECURITY FUNDAMENTAL ELEMENTS 17

5.1 IDENTIFICATION 17

5.1.1. Identification and classification 18

5.1.2. Interconnections 18

5.1.3. Assets Management 19

5.1.4. Risk Management 19

5.2 PROTECTION 20

5.2.1. Identity and Access Management 20

5.2.2. Security Awareness and Training 21

5.2.3. Human Resource Security 21

5.2.4. Network and Infrastructure Management 22

5.2.5. Systems Acquisition and Development 23

5.2.6. Change and Patch Management 25

5.3 DETECTION 26

5.3.1. Anomalies and Events 26

5.4 TESTING 27

5.4.1. Vulnerability Management 27
5.4.2. Scenario-Based Testing 28
5.4.3. Penetration Tests 29
5.4.4. Red-Team Testing 29
5.5 RESPONSE AND RECOVERY 29
5.5.1. Cyber-resilience Incident Management 29
5.5.2. Data Integrity 31
5.5.3. Communication and Collaboration 31
5.5.4. Crisis Communication and Responsible Disclosure 32
5.5.5. Supply Chain and Dependency Management 33
5.5.6. Cyber Threat Intelligence 33
5.5.7. Information Sharing 35
5.5.8. Incident Notification 35
5.5.9. Comprehensive testing programme 36
6. REMEDIAL MEASURES AND ADMINISTRATIVE SANCTIONS 36
7. APPENDIX 37
7.1 Appendix A: Cybersecurity Incident Reporting Form 37

1. AUTHORITY, PURPOSE AND SCOPE

1.1 Authority

These guidelines are issued by the Tanzania Cooperative Development Commission (TCDC), pursuant to its authority set forth in Cooperative Society Act, 2013 and the Microfinance Act, 2018.

These Guidelines shall be referred to as the **Cybersecurity Guideline for Savings and Credit Cooperative Societies (SACCOS) No. 1 of 2024**, shall come into force on 1st November 2024, and are hereby issued by the Tanzania Cooperative Development Commission (TCDC).

These Cybersecurity guidelines seek to provide SACCOS with guiding principles that are consistent with local and international best practices, for establishing adequate cybersecurity frameworks to ensure cyber resilience. The cyber security framework to be established should be proportional to the SACCOS business model, complexity of operations

1.2 Applicability

All SACCOS regulated by the Tanzania Cooperative Development Commission under the Cooperative Society Act, 2013, the Microfinance Act, 2018 and its regulations as well as other available legislations in the country are expected to comply and implement these guidelines in order to ensure cyber resilience in SACCOS.

1.3 Scope of Authority

These guidelines apply to SACCOS registered and licensed under the Cooperative Society Act, 2013, and the Microfinance Act, 2018. In implanting the guidelines, SACCOS are expected to use a risk-based approach by evaluating their current environments, identifying gaps and prioritizing mitigation of identified high risks. In addition, SACCOS should consider the following:

a) Process for compliance: SACCOS must send their self-assessment against the guidelines to the TCDC within 90 days from the date of issue of the guidelines, and subsequently by December 31 each year.
b) Proportionality- all SACCOS should comply with the provisions set out in the guidelines in such a way that is proportionate to, and takes account of, the size,

internal organization, complexity and risk of the SACCOS' operations and information and communication technology (ICT).

c) Incident reports- a SACCOS must report, in the form and manner determined by the SACCO, any material systems failure, malfunction, delay or other disruptive event or cyber incident, that are classified as material, within 48 hours of occurrence.
d) Classification- any questions that arise as to the interpretation and application of the guidelines should be addressed to Registrar.

2. INTRODUCTION

Cyber-attacks are increasing in frequency, sophistication and impact, with perpetrators continually refining their efforts to compromise systems, networks and information world-wide. The SACCOS sector is one of the prime targets for such attacks, given the intensive use of technology in the sector.

Therefore, the TCDC has developed these cybersecurity and resilience guidelines in order to raise awareness and promote the governance and management of cyber risk within the sector. The guidelines are based on the International Organisation for Standardisation/International Electrotechnical Commission (ISO/IEC 27001), Control Objectives for Information and Related Technology (COBIT 5) , The National Institute of Standards Cybersecurity Framework (NIST CSF), Information Security Forum's Standard of Good Practice for Information Security (ISF), and international best practices, and seek to set out requirements for SACCOS sector to improve their cyber-resilience posture.

The guidelines primary serves as an overarching framework for the governance and management of cyber risk, which SACCOS can tailor to their own specific needs and technologies, taking into account the principle of proportionality.

The key components of the guidelines comprise the following:

a) Governance: Cyber governance refers to the arrangements a SACCO has put in place to establish, implement and review its approach to managing cyber risks. Effective cyber governance should start with a clear comprehensive cyber-resilience framework that prioritises the security and efficiency of a SACCO operations and supports financial stability objectives. The framework should be guided by a SACCO cyber-resilience strategy, define how the SACCO's cyber-resilience objectives are determined, and outline its people, processes and technology requirements for

managing cyber risks and timely communication, in order to enable a SACCO to collaborate with relevant stakeholders to effectively respond to and recover from cyber incidents. The framework should be supported by clearly defined roles and responsibilities of the board and senior management of the SACCO. The board and senior management should cultivate a culture that ensures a high level of accountability by staff at all levels regarding effective cyber resilience.

b) Identification: given that a SACCO's operational failure can negatively affect financial stability, it is crucial that SACCOS identify which of their critical operations and supporting information assets should, in order of priority, be protected against compromise. After the identification or asset classification process, the SACCO must have a robust risk assessment process in place to determine the criticality of its assets and how to protect them using a variety of controls.

c) Protection: a SACCO's ability to implement effective security controls and system process designs that protect the confidentiality, integrity, and availability of its assets and services.

d) Detection: A SACCO's ability to recognise signs of a potential cyber incident or detect breach incidents is essential to strong cyber resilience. Early detection of cyber incidents provides a SACCO with useful lead time to mount appropriate countermeasures against a potential breach and allows proactive containment of actual breaches.

e) Testing is an integral component of any cyber resilience framework. All elements of a cyber resilience framework should be rigorously tested to determine their overall effectiveness before being deployed within SACCOS, and regularly thereafter. This includes the extent to which the framework is implemented correctly, operating as intended and producing desired outcomes. Understanding the overall effectiveness of the cyber resilience framework in the SACCOS and its environment is essential in determining the residual cyber risk to SACCOS operations, assets, and ecosystem. Sound testing regimes produce findings that are used to identify gaps in stated resilience objectives and provide credible and meaningful inputs to the SACCOS cyber risk management process. Analysis of testing results provides direction on how to correct weaknesses or deficiencies in the cyber resilience posture and reduce or eliminate identified gaps. The scope of testing for the purpose of this guidance

includes vulnerability assessments, scenario-based testing, penetration tests and tests using red teams.

3. DEFINITION OF TERMINOLOGY

In this Guideline:

Access control	To ensure that access to assets is authorized and restricted, having regard to business and security requirements.
Advanced persistent threat (APT)	A threat actor that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple threat vectors. The APT pursues its objectives repeatedly over an extended period of time, adapts to defenders' efforts to resist it, and is determined to execute its objectives.
Asset	Something of either tangible or intangible value that is worth protecting, including personnel, information, infrastructure, finance and reputation.
Authenticity	A property that an entity is what it claims to be.
Availability	Property of being accessible and usable on demand by an authorised entity.
Blue team	A team that evaluates organisational security environments and defends these environments from red teams.
Campaign	A grouping of coordinated adversarial behaviours that describe a set of malicious activities that occur over a period of time against one or more specific targets.
Compromise	Violation of the security of an information system.
Confidentiality	Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems.
Course of action (Coa)	An action or actions taken to either prevent or respond to a cyber incident.
Cyber	Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.
Cyber alert	Notification that a specific cyber incident has occurred or a cyber threat has been directed at an organisation's information systems.
Cyber event	Any observable cyber occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.

Cyber incident	A cyber event that jeopardises the cyber security of an information system or the information the system processes, stores or transmits; or violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.
incident Response plan	Procedures to respond to and limit consequences of a cyber
Cyber resilience	The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.
Cybersecurity risk	The combination of the probability of cyber incidents occurring and their impact.
Cyber security	Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium.
Cyber threat	A circumstance with the potential to exploit one or more vulnerabilities that can adversely affect cybersecurity.
Data breach	Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data transmitted, stored or otherwise processed.
Defence-in-depth	Security strategy integrating human resources, processes and technology to establish a variety of barriers across multiple layers and dimensions of an organisation.
Denial of service (DoS)	Prevention of authorised access to information or information systems, or the delaying of information system operations and functions, with a resultant loss of availability to authorised users.
Detection (function)	Develop and implement the appropriate activities to identify the occurrence of a cyber event.
Distributed denial of service (DDoS)	A denial of service that is carried out using numerous sources simultaneously.
Exploit	Defined way to breach the security of information systems through vulnerability.
Identification (function)	Develop an organisational understanding to manage cyber risk to assets and capabilities.
Incident response team (IRT)	Team of appropriately skilled and trusted members of the organisation that handles incidents during their life cycle.
Indicators of compromise (IoC)	Identifying signs that a cyber incident may have occurred or may be occurring.
Information sharing	An exchange of data, information and/or knowledge that can be used to manage risks or respond to events.

Information system	A set of applications, services, information technology assets or other information-handling components, which includes the operating environment.
Integrity	Property of accuracy and completeness.
Logical access	Providing an authorised user the ability to access one or more computer-system resources such as a workstation, network, application, or database through automated tools.
Malware	Software designed with malicious intent, containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems.
Material incident	Any incident that is considered to have a major or significant impact on the operations of an institution and is likely to cause potential systemic failures.
Multi-factor authentication	The use of two or more of the following factors to verify a user's identity: knowledge factor, possession factor and biometric factor.
Non-repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities.
Patch management:	The systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes and service packs.
Penetration testing	A test methodology in which assessors, using all available documentation (for example, system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
Protection (function)	To develop and implement appropriate safeguards to ensure delivery of services and to limit or contain the impact of cyber incidents.
Recover (function)	To develop and implement the appropriate activities to maintain plans for cyber resilience and to restore any capabilities or services that were impaired by a cyber incident.
Recovery-point objectives (RPOs)	Refers to the amount of data that can be lost within a period most relevant to a business, before significant harm occurs, from the point of a critical event to the most preceding backup.
Recovery-time objectives (RTOs)	The amount of time that an application, system or process, can be down for without causing significant damage to the business as well as the time spent restoring the application and its data.
Reliability	Property of consistent intended behaviour and results.

Respond (function)	To develop and implement the appropriate activities to respond to a detected cyber event.a level of understanding that is relevant to act upon in mitigating the impact of a potentially harmful event.
Social engineering	A general term for trying to deceive people into revealing information or performing certain actions.
Tactics, techniques and procedures (TTPs)	The behaviour of a threat actor. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.
Threat actor	An individual, a group or an organisation believed to be operating with malicious intent.
Threat assessment	Process of formally evaluating the degree of threat to an organisation and describing the nature of the threat.
Threat intelligence	Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision- making processes.
Threat-led penetration testing (TLPT) (also known as red team testing)	A controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques, and procedures of real-life threat actors. It is based on targeted threat intelligence and focusses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations.
Threat vector	A path or route used by the threat actor to gain access to the target.
Verification	A confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.
Vulnerability	A weakness, susceptibility, or flaw of an asset or control that can be exploited by one or more threats.
Vulnerability assessment	A systematic examination of an information system and its controls and processes to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

4. CYBER RISK MANAGEMENT AND OVERSIGHT

4.1 GOVERNANCE

Cyber governance refers to the arrangements SACCOS has put in place to establish, implement, and review its approach to managing cyber risks. Effective cyber governance should start with a clear and comprehensive cyber resilience framework that prioritizes the security and efficiency of the SACCOS operations and supports business stability objectives.

4.1.1. Oversight

TCDC shall conduct oversight inspections to SACCOS to assess the adequacy of cyber resilience. The inspections would be based on the requirements provided and other assessment processes developed from time to time in order to test available systems vulnerability, advice, protect and mitigate cyber-attacks.

4.1.2. Cyber-Resilience Strategy

a) The framework should be guided by SACCOS cyber resilience strategy, define how the SACCOS cyber resilience objectives are determined, and outline its people, processes, and technology requirements for managing cyber risks and timely communication, in order to enable SACCOS to collaborate with relevant stakeholders to effectively respond to and recover from cyber-attacks.

b) It is essential that the framework is supported by clearly defined roles and responsibilities of the SACCOS board and its management, and it is incumbent upon its board and management to create a culture which recognizes that staff at all levels have important responsibilities in ensuring SACCOS cyber resilience.

c) Strong cyber governance is essential to SACCOS implementation of a systematic and proactive approach to managing the prevailing and emerging cyber threats that it faces. It also supports efforts to appropriately consider and manage cyber risks at all levels within SACCOS and to provide appropriate resources and expertise to deal with these risks.

4.1.3. Cyber-Resilience Framework

a) SACCOS should have a framework that clearly articulates how it determines its cyber resilience objectives and cyber risk as well as how it effectively identifies, mitigates and manages its cyber risks to support its objectives.

b) SACCOS board should endorse this framework, ensuring it is aligned with the SACCOS formulated cyber resilience strategy. The SACCOS cyber resilience framework should support business stability objectives while ensuring the ongoing efficiency, effectiveness, and economic viability of its services to its users. Therefore, framework objectives should aim to maintain and promote SACCOS ability to anticipate, withstand, contain, and recover from cyber-attacks, to limit the likelihood or impact of a successful cyber-attack on its operations or on the broader financial system. The SACCOS cyber resilience framework should be reviewed and updated periodically to ensure that it remains relevant.

c) Cyber is more than just ICT. The strategies and measures to SACCOS cyber resilience framework should not be restricted to securing the viability of its information technology operations alone but should also cover environment, people, and processes. The framework should, in addition, include timely communication to enable SACCOS to collaborate with relevant stakeholders (i.e. Forensic investigators and System Auditors) to effectively respond to and recover from cyber-attacks.

d) The SACCOS cyber resilience framework should be consistent with its enterprise operational risk management framework. Such consistency is important and recognizes that a SACCOS cyber resilience framework is likely to share common elements with the policies, procedures, and controls that it has established to manage other areas of risks. For example, limiting physical access can be a key control to address the risk to critical ICT infrastructure.

e) SACCOS should take an integrated and comprehensive view of the potential cyber threats it faces. SACCOS cyber resilience framework should consider how the SACCOS would regularly review and actively mitigate the cyber risks that it bears from and poses to its participants, other SACCOS, vendors, vendor products and its service providers, which are collectively referred to in this document as a SACCOS ecosystem.

f) There are many relevant international, national, and industry-level standards, guidelines, or recommendations that SACCOS could use as a benchmark in designing its cyber resilience framework. Given SACCOS systemic importance, they should align themselves with leading standards, guidelines, or recommendations, reflecting current industry best approaches in managing cyber threats, and incorporate the most effective cyber resilience solutions.

g) SACCOS cyber resilience framework should clearly define the roles and responsibilities including accountability for decision making within SACCOS for managing cyber risk, including in emergencies and in a crisis.

h) SACCOS internal processes should help the board and senior management assess and measure the adequacy and effectiveness of the SACCOS cyber resilience framework. The adequacy of and adherence to SACCOS cyber resilience framework should be assessed and measured regularly through independent compliance programmes and audits carried out by qualified individuals. To assess and measure the effectiveness of its cyber resilience framework, SACCOS is encouraged to use relevant models as well as the results of its testing programmes.

4.1.4. Board and Senior Management Responsibilities

The board and senior management are responsible for ensuring that cyber-security risk is effectively managed within the SACCO.

The board should

a) Be responsible for approving a cyber-resilience strategy and framework, setting a SACCOS' risk tolerance for cybersecurity risks and closely overseeing the SACCOS' implementation of its cyber-resilience framework and the policies, procedures and controls that support it.
b) Be regularly apprised of a SACCO's cyber-security risk profile to ensure that it remains consistent with the SACCO's risk tolerance and overall business objectives. As the board shares this responsibility, it should consider how material changes to the SACCO's products, services, policies or practices, and the threat landscape affect its cyber-risk profile.

To carry out the foregoing responsibilities, a SACCO's board should ensure that it collectively possesses the appropriate balance of skills, knowledge and experience to

understand and assess the cyber-security risks facing the SACCO. It should also be sufficiently informed and capable of credibly challenging the recommendations and decisions of designated senior management.

Senior management should

a) Closely oversee a SACCOS' implementation of its cyber-resilience framework, and the policies, procedures and controls that support it.
b) Cultivate a strong level of awareness and commitment to cyber resilience. An institution's senior management should promote a culture that recognises that staff at all levels have important responsibilities for ensuring the institution's cyber resilience and lead by example.
c) Ensure that behavioural and cultural change is nurtured and conveyed through leadership and vision with clear and effective messages.
d) Ensure that situational awareness materials are made available to relevant employees to mitigate cyber incidents, changes to the threat landscape and effects of these threats on the institution.
e) Ensure that a cyber-security function is established. The function must be independent of an institution's information technology function; to avoid any conflict, the cyber-security function must have a separate reporting function from the information technology function, separate budget and resources.
f) Ensure that a consultant for the cyber-security function, is appointed by the SACCO. The Cybersecurity consultant should be independent, possess an appropriate balance of skills, knowledge and experience, and have sufficient resources and direct access to the board. In addition, The Cybersecurity consultant should be responsible and accountable for implementing the cyber-resilience strategy and framework at the enterprise level.
g) Develop key performance indicators, key risk measures and ensure supporting data is routinely collected at senior management level to monitor, measure and report on the implementation, effectiveness, consistency and persistence of cyber activities within an institution, the group and local financial system.
h) Ensure the standard board information pack includes a report and metrics that cover cybersecurity. Sufficient time must be allocated to discuss issues on the board agenda.
i) Ensure that an independent risk management function exists at an enterprise level. An independent risk management function ensures that the cyber-risk management framework has been implemented according to policy and consistently to an

institution's risk appetite and tolerance. In addition, an independent risk management function reports significant changes in an institution's risk exposure to the appropriate governing authority.

j) Ensure that an independent audit function exists at an enterprise level. An independent audit function ensures the effective functioning of internal controls and applicable laws and regulations; updates its procedures to adjust to the evolving cyber threat landscape; and identifies, tracks, and reports significant changes in an institution's cyber-risk exposure to the appropriate governing authority.

k) Establish processes to identify and communicate all cyber-security-related regulations and requirements. The process for ensuring compliance should be reviewed and updated when new regulatory requirements become effective. The regulatory compliance process should address compliance with the following:

i. payment card industry, data security standard (PCI-DSS)

ii. electronic communications and transactions regulations

iii. electronic evidence regulations

iv. Data Protection Act, Act No. 1 of 2023

v. Cybercrime Act, 2015, and all other laws governing protection, integrity and availability of critical assets.

5. CYBER-SECURITY FUNDAMENTAL ELEMENTS

5.1 IDENTIFICATION

Given that SACCOS operational failure can negatively affect business stability, it is crucial for the SACCOS to identify its critical operations and information assets that should be protected against cyber-attack. The ability of SACCOS to understand its internal situation and external dependencies is key to being able to effectively respond to potential cyber threats that might occur. This requires SACCOS to know its information assets and understand its processes, procedures, systems and other dependencies to strengthen its overall cyber resilience posture.

5.1.1. Identification and classification

a) SACCOS should identify its business functions and supporting processes and conduct a risk assessment to ensure that it carefully understands the importance of each function and supporting processes, and their interdependencies, in performing its functions. Identified business functions and processes should then be classified in terms of criticality, which in turn should guide the financial institution's prioritization of its protective, detective, response, and recovery efforts.

b) Similarly, a SACCOS should identify and maintain a current inventory of its information assets and system configurations, including interconnections with other internal and external systems, to know at all times, the assets that support its business functions and processes. SACCOS should carry out a risk assessment of those assets and classify them in terms of criticality. It should identify and maintain a current log of both individual and system usernames to know the access rights to information assets and their supporting systems and should use this information to facilitate identification and investigation of anomalous activities.

c) SACCOS should integrate identification efforts with other relevant processes, such as acquisition and change management, in order to facilitate a regular review of its list of critical business processes, functions, individual and system credentials and its inventory of information assets so that they remain current, accurate and complete.

5.1.2. Interconnections

a) SACCOS systems and processes are directly or indirectly interconnected with other systems and processes of the entities within its ecosystem, e.g. participants, linked SACCOS settlement banks, liquidity providers, service providers, critical infrastructure such as energy and telecommunications, vendors, and vendor products.

b) Consequently, the cyber resilience of those entities could have significant implications in terms of the cyber risk that the SACCOS faces, particularly since the significance of the risks they may pose is not necessarily proportionate to the criticality of their business relationship with the SACCOS.

c) Therefore, SACCOS should identify the cyber risks that it bears from and poses to entities in its ecosystem and coordinate with relevant entities, as appropriate, as they design and implement resilience efforts with the objective of improving the overall resilience of the ecosystem.

5.1.3. Assets Management

The SACCO should

a) Maintain up-to-date inventory of all the critical functions; key roles; processes; information assets; third-party service providers and interconnections; and, where possible, automated tools should be used for this purpose. In determining the criticality of the information assets, an institution should at a minimum consider the confidentiality, integrity and availability principles of information security.

b) Create and maintain a simplified network map of resources with an associated plan addressing internet protocol address, which locate routing, and security services and servers supporting critical functions, and which identify links with the outside world.

c) Maintain a comprehensive inventory of all individuals and systems accounts so that they can be aware of the access rights to information assets and their supporting systems; the inventory must be reviewed and updated regularly.

d) Maintain up-to-date and complete maps of network resources, interconnections and dependencies, and data flows with other information assets, including the connections to business partners, internet-facing services, cloud services and any other third-party systems.

5.1.4. Risk Management

e) SACCOS should actively monitor technological developments and keep abreast of new cyber risk management processes that can effectively counter existing and newly developed forms of cyber-attack. SACCOS should consider acquiring such technology and know-how to maintain its cyber resilience.

f) SACCOS cyber risk management practices should go beyond reactive controls and include proactive protection against future cyber events. Predictive capabilities and anticipation of future cyber events are based on analysing activity that deviates from the baseline. SACCOS should work towards achieving sources and capabilities, capturing data from multiple internal and external sources, and defining a baseline for behavioural and system activity.

5.2 PROTECTION

Cyber resilience depends on effective security controls and system and process design that protect the confidentiality, integrity and availability of SACCOS assets and services. These measures should be proportionate to SACCOS threat landscape and systemic role in the business system, and consistent with its risk tolerance.

The SACCO should consider the following measures to address the requirements of the protection function:

5.2.1. Identity and Access Management

The SACCO should

a) identify and restrict physical and logical access to its system resources to the minimum required for legitimate and approved work activities, according to the principle of least privilege and separation of duties.

b) Establish policies, procedures and controls that address access privileges and how that access should be administered. The information system access should be evaluated regularly to identify unneeded access or privileges. Physical, logical and remote access to critical systems should restrict and block any unauthorized access. Administration rights on systems should be strictly limited to operational needs.

c) Establish and administer user accounts in accordance with a role-based access control (RBAC) scheme that organizes allowed information system access rights and privileges into roles.

d) Establish processes to manage the creation, modification or deletion of user access rights, such actions should be submitted to and approved by appropriate staff and should be recorded for review if necessary.

e) Implement specific procedures to allocate privilege access on a need-to-use or an event-by-event basis. Administrators should have two types of accounts: one for general purpose use and one to carry out their administrative tasks. The use of privileged accounts should be tightly monitored and controlled.

5.2.2. Security Awareness and Training

The SACCO should

a) Ensure that its employees have a good understanding of the cyber-security risk they might face when performing their jobs and that they understand their roles and responsibilities in protecting the institution's assets.

b) Provide its entire staff (permanent employees, temporary employees and contractors) with training to support cyber-security-policy compliance and the incident-reporting process. Training should include good practices for dealing with potential cyber incidents, including how to report unusual activity. Cyber-security awareness training should be part of the on-boarding programmes for new staff.

c) Ensure that before going into service operations, staff operating new systems should receive appropriate user training and be familiar with the operating procedures.

d) Should validate the effectiveness of its training, assess whether the training and awareness positively influence behavior and ensure that staff comply with the operating procedures. High-risk staff should be identified and receive dedicated security-awareness training that is relevant to their responsibilities.

5.2.3. Human Resource Security

The SACCO should

a) Embed cybersecurity at each stage of the employment life cycle, specifying security-related action required during the induction of each employee and their ongoing management, and upon the termination of employment.

b) Carry out background security vetting of all candidates that is commensurate with their future role and depending on the criticality of the assets and information they might have access to in order to fulfil their duty. Responsibilities for cybersecurity should be clearly stated in employment contractual agreements.

c) Establish policies, procedures and controls for granting or revoking employees' physical and logical access to its systems, considering job responsibilities, principles of least privilege and segregation of duties.

d) Establish capabilities, including people, processes and technologies to monitor privileged user activity and access to critical systems in order to identify and deter anomalous behavior and notify appropriate staff.

e) Monitor and analyze behavior to identify anomalous activities and evaluate the implementation of innovative solutions to support detection and response to insider threat activity.

f) Ensure that all access rights that are related to employees' previous position and are no longer necessary for their new responsibilities are revoked when employee responsibilities change. Employees in sensitive positions should be pre-screened to ensure due diligence and to protect the institution's information assets.

g) Senior management should ensure that the institution's cultural awareness of cyber-security risk improves continuously across the organisation and its ecosystem. In addition, institutions should develop key indicators to measure the effectiveness of training programmes to ensure that there are updated regularly to take account of the evolving threat landscape to the ecosystem.

5.2.4. Network and Infrastructure Management

The SACCO should

a) implement a defence-in-depth security architecture based on the network and data flow diagrams that identify hardware, software and network components, internal and external connections and type of information exchanged between systems.

b) Establish a baseline system and security configuration for information systems and system components, including devices used for accessing an institution's network remotely, to help the configuration and security reinforcements of those systems and components to be applied consistently. These baselines should be documented, formally reviewed and regularly updated to adapt to the institution's evolving threat landscape.

c) Segment its network infrastructure with security policies appropriate to its use and commensurate with the risk score, which defines proper access policy to systems and applications. Sensitive traffic between systems and zones should be segregated using network management.

d) Implement technical measures to prevent the execution of unauthorized code on institution-owned or managed devices, network infrastructure and system components and unauthorized devices should be prevented from connecting to the institution's networks.

e) Develop appropriate controls to protect data at rest, in use and in transit. The controls should be commensurate with the criticality and the sensitivity of the data held, used or being transmitted, according to the risk assessment conducted in the identification function.

5.2.5. Systems Acquisition and Development

The SACCO should

a) Develop and implement a process governing the acquisition, development and maintenance of ICT systems; this process should be designed using a risk-based approach.

b) Ensure that, before any acquisition or development of ICT systems takes place, the functional and non-functional requirements (including information security requirements) are clearly defined and approved by the relevant business management.

c) Ensure that measures are in place to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development and implementation in the production environment.

d) Have a method in place for testing and approving ICT systems before their first use; the method should consider the criticality of business processes and assets. The testing should ensure that new ICT systems perform as intended. The institution should also use test environments that adequately reflect the production environment.

e) Test ICT systems, ICT services and information security measures to identify potential security weaknesses, violations and incidents.

f) implement separate ICT environments to ensure adequate segregation of duties and to mitigate the impact of unverified changes to production systems.

g) Specifically, a financial institution should ensure the segregation of production environments from development, testing and other non-production environments.

h) Ensure the integrity and confidentiality of production data in non-production environments. Access to production data is restricted to authorized users.

i) Implement measures to protect the integrity of the source codes of ICT systems that are developed in-house. They should also document the development, implementation, operation or configuration of the ICT systems comprehensively to reduce any unnecessary dependence on subject experts. Documentation of the ICT system should contain, where applicable, at least user documentation, technical system documentation and operating procedures.

SACCO’s processes for acquisition and development of ICT systems should also apply to ICT systems developed or managed by the business function's end users outside the ICT organisation (for example, end-user computing applications) using a risk-based approach. The financial institutions should maintain a register of these applications that support critical business functions or processes.

5.2.6. Change and Patch Management

The SACCO should have policies, procedures and controls for change management, which should include criteria for prioritising and classifying the changes. Before any change, the SACCO should ensure that the change request is:

a) Reviewed to ensure that it meets business needs.
b) Categorized and assessed for identifying potential risks and to ensure that it will not negatively affect confidentiality, integrity and availability as well as the SACCO's systems and data.
c) Approved before it is implemented by the appropriate level of management.
d) The change management process should be based on well-established and industry-recognized standards and best practices, for example COBIT 5.
e) An entity should consider building a segregated or separate environment that mirrors the production environment, allowing rapid testing and changes and patches to be implemented, and for providing for rapid fall-back when needed.

The SACCO should

a) Have a comprehensive patch management policy and process that includes maintaining current knowledge of available patches, identifying appropriate patches for particular systems and analyzing impacts if installed, ensuring that patches are installed properly (for example, by applying the four-eyes principle) and tested prior to and monitored after installation, and documenting all associated procedures, such as specific configurations required. Policies, procedures and controls must make use of the information from the asset inventory management.

b) Process described in the identification phase that provides information on the installed programs and binaries.

c) Ensure that installation of new patches have approval from the appropriate management level.

d) Have necessary procedures for recovering quickly when changes or patches fail. Any changes to the production environment must have an associated contingency plan,

where applicable, and have policies and procedures to prohibit unapproved changes and patch installation to the information system.

5.3 DETECTION

5.3.1. Anomalies and Events

The SACCO should

a) Develop appropriate capabilities, including personnel, processes and technology, to monitor and detect, in time, anomalous activities and events by setting appropriate criteria, indicators and triggers to enable alerts; the institution should understand the potential impact of the events.

b) Use the results of the risk assessment performed in the identity function to define, consider and document the baseline profile of system activities to help detect deviation from the baseline.

c) Ensure that its relevant staff are trained to be able to identify and report anomalous activities and events, and that roles and responsibilities for detection are well deflned to ensure accountability.

d) Develop and implement a mechanism that correlates all the network and systems alerts, and anomalous activity across its business units to detect multifaceted attacks. A process to collect, centralize and correlate event information from multiple sources and log analysis to continuously monitor the environment and detect anomalous activities and events should be established.

e) Continuously monitor and inspect network traffic, including remote connections, endpoint configuration and activity, to identify potential vulnerabilities or anomalous events promptly.

f) Continuously monitor connections with external service providers, devices and software.

The SACCO's monitoring and detection capabilities should support information collection for forensic investigation. To facilitate forensic investigation, the SACCO should ensure that its logs are backed up at a secure location with controls, to mitigate the risk of alteration.

5.4 TESTING

a) Any SACCO requires a framework for testing cyber resilience; thus, the SACCO should establish and maintain a comprehensive testing programmes as an integral part of its cyber-resilience framework. The testing programmes should consist of a broad spectrum of methodologies, practices and tools for monitoring, assessing and evaluating the effectiveness of the core components of the cyber-resilience framework.

b) SACCO should incorporate risk-based elements in developing the comprehensive testing programmes. This should be reviewed and updated regularly, taking account of the evolving threat landscape and the criticality of assets.

c) Tests should be undertaken by independent parties, whether internal or external.

d) The SACCO’s board and senior management should incorporate lessons from th test results into the cyber-resilience framework to continually improve its cyber-resilience posture.

e) The SACCO should regularly, at least annually, test critical systems, applications and data recovery plans.

5.4.1. Vulnerability Management

a) SACCO should develop a documented and regularly updated vulnerability management process to classify, prioritize and remedy potential weaknesses identified at the stage of vulnerability assessments and perform subsequent validation to assess whether gaps have been fully addressed.

b) The vulnerability management programmes should identify any type of exploitable weakness in critical functions.

c) SACCO should conduct vulnerability scanning for its external-facing services and internal systems and networks periodically. Vulnerability assessments should be performed before any deployment or redeployment of new or existing services supporting critical functions, applications and infrastructure components for fixing weaknesses, consistently with existing change and release management processes. This vulnerability assessment should be done by a company registered and licensed by TCDC to provide ICT consultation service.

The SACCO should

a) Develop, monitor and analyze metrics to assess the performance and effectiveness of its vulnerability management programmes.
b) Consider discussing relevant test conclusions with TCDC to boost the cyber resilience of its ecosystem and the SACCOS sector as a whole, as far as possible and under specific information-sharing arrangements.
c) Conduct quarterly vulnerability assessments on running services, applications and infrastructure components for compliance checks against regulations, policy and configurations, as well as for monitoring and evaluating the effectiveness of security controls to address the identified vulnerabilities.

5.4.2. Scenario-Based Testing

a) The SACCO should perform different scenario-based tests, including extreme but plausible scenarios, to evaluate and improve its incident-detection capability, as well as response, resumption and recovery plans. Scenario-based tests can take the form of desktop exercises or simulations.
b) The SACCO's board and senior management should be engaged in the scenario-based test, when appropriate, to have them aware of the threat landscape and be able to reach risk-based decisions relating to, among others, resources and processes required to mitigate cyber threats.
c) To improve an institution's staff awareness and enhance the risk culture within an organisation, scenario-based tests should include social engineering and phishing simulation.
d) The SACCO should test the extent to which internal skills, processes and procedures can adequately respond to extreme but plausible scenarios, with a view to achieving stronger operational resilience.
e) The SACCO should form collaborative arrangements with the ecosystem to develop cybersecurity-incident scenarios involving significant financial loss and use them for

stress tests to better understand potential spillovers and contagion risk to the ecosystem. The stress-test results should be used to further improve the institution's cyber-resilience stance.

5.4.3. Penetration Tests

The SACCO should

f) Conduct penetration tests on its external-facing services and internal systems and networks to identify vulnerabilities in the adopted technology, organisation and operations regularly, or at least on an annual basis. Penetration tests should be conducted using a risk-based approach and, at the very least, in cases of major changes and new system deployment.
g) Perform penetration tests engaging all critical internal and external stakeholders in the penetration-testing exercises: system owners, business continuity, and incident and crisis response teams.
h) Design and perform penetration tests to simulate realistic attack techniques on systems, networks, applications and procedures.

5.4.4. Red-Team Testing

The SACCO should conduct Red-Team exercises to test critical functions for possible vulnerabilities and the effectiveness of an institution's mitigating controls, including controls relating to protection of personnel, processes and technology. It should also conduct independent red-team exercises, using regulatory and industry frameworks. This should be done by licensed service provider by TCDC to provide such services to SACCOS.

5.5 RESPONSE AND RECOVERY

Business stability may depend on SACCOS ability to settle obligations when they are due. Therefore, SACCOS arrangements should be designed to enable it to resume critical operations rapidly, safely and with accurate data to mitigate the potentially systemic risks of failure to meet such obligations when participants are expecting it to meet them.

5.5.1. Cyber-resilience Incident Management

a) The SACCO should develop a comprehensive cyber-incident response, resumption and recovery plans to manage cybersecurity events or incidents in a way that limits

damage and priorities resumption and recovery actions to facilitate the processing of critical transactions, increase the confidence of external stakeholders, and reduces recovery time and costs. Such plans should define policies and procedures as well as roles and responsibilities of escalating, responding to, and recovering from cyber-security incidents. An institution should ensure that all relevant business units are integrated into the plans.

b) The cyber-incident response, resumption and recovery processes should be closely integrated with crisis management, business continuity, and disaster recovery planning and recovery operations.

The SACCO should

a) Ensure that its incident response team has the requisite skills and training to address cyber incidents.
b) After consideration of its critical function, key roles, processes, information assets, third-party service providers and interconnections, plan for how to operate in a diminished capacity or how to safely restore services over time, taking into consideration the relative priorities of services affected by the incident, and with accurate data. To make the best decisions about its recovery objectives after a cyber incident, an institution must first define its recovery-point objectives (RPOs) and its recovery-time objectives (RTOs) commensurate with its business needs and systemic role in the ecosystem.
c) Regularly (quarterly) test its cyber contingency, response, resumption and recovery plans against a range of different plausible scenarios.
d) Define alert indicators and thresholds for detecting cyber-security incidents that trigger the incident management processes and procedures, which, in turn, include alerting and conveying information to the appropriate staff.
e) Have processes and procedures for collating and reviewing information from its cyber-security incidents and testing results in order to continuously improve its contingency, response, resumption and recovery plans.
f) Have processes and procedures to conduct an ex-post root-cause analysis of its cyber-security incidents. Findings of the root-cause analysis should be incorporated into the cyber response, resumption and recovery plans.

5.5.2. Data Integrity

The SACCO should

a) Develop a formal backup policy specifying the minimum frequency and scope of data, taking into consideration data sensitivity and the frequency with which that new information is introduced.
b) Develop backup and recovery methods and strategies to be able to restore system operations with minimum downtime and limited disruption.
c) Regularly back up all data necessary to replay participants' transactions.
d) Store backup copies at an alternate site with a different risk profile to the main site and with transfer rates consistent with actual RPOs. The alternate site and backups should be safeguarded by stringent protective and detective controls.
e) Back up its information system by maintaining a redundant secondary system that is not located in the same place as the primary system and that can be activated without information being lost or operations disrupted.
f) Consider having a data-sharing agreement with third parties or participants to obtain uncorrupted accurate data from them for recovering its business operations in a timely manner.
g) Backups should be protected at rest and in transit to ensure the confidentiality, integrity and availability of data. Backups should be tested regularly to verify their availability and integrity.

5.5.3. Communication and Collaboration

The SACCO should

(a) identify, document and regularly review systems and processes supporting its critical functions or operations that are dependent on external connectivity.
(b) develop policies and procedures that define how it should work together with relevant interconnected entities to enable operations to be resumed (priority being its critical functions and services) as soon as it is safe and practicable to do so.
(c) closely cooperate with its interconnected entities within the ecosystem, establishing roll-back processes to restore all its services accurately and safely. Moreover, an institution should test the effectiveness of these procedures regularly.

(d) design its network connection infrastructure in a way that allows connections to be segmented or severed instantly to prevent contagion arising from cyber-attacks.

5.5.4. Crisis Communication and Responsible Disclosure

This section discusses how a cyber-incident communication plan is developed and what elements are included in the plan, how information is collected in the field, analyzed, and eventually disseminated to internal and external stakeholders in the media world that is evolving.

The SACCO should

(a) Identify and determine staff who are essential for mitigating the risk of a cyber incident and make them aware of their roles and responsibilities regarding incident escalation.

(b) Establish criteria and procedures for escalating cyber incidents or vulnerabilities to the board and senior management, taking account of the potential impact and criticality of the risk.

(c) Have a communication plan and procedures to notify, as required or necessary, all relevant internal and external stakeholders (including oversight, regulatory authorities, media and customers) promptly when it becomes aware of a cyber incident or when a cyber incident occurs. Incident reporting to the Bank of Tanzania should be within 48 hours from detecting the incident.

(d) Have a policy and procedures to enable potential vulnerabilities to be disclosed responsibly. In particular, it should prioritise disclosures that could help stakeholders to respond promptly and mitigate risk, which could benefit the ecosystem and broader financial stability.

(e) Establish and regularly review information-sharing rules, agreements and modalities to control the publication and distribution of information that may have adverse consequences if disclosed.

(f) At least annually, test response, resumption and recovery plans, including governance and coordination, and crisis communication arrangements and practices. The incident response plan should identify the internal and external

stakeholders that must be notified, as well as the information that has to be shared and reported, and when this should take place.

The incident response plan should identify the internal and external stakeholders that must be notified, as well as the information that has to be shared and reported, and when this should take place.

5.5.5. Supply Chain and Dependency Management

(a) The SACCO should maintain and regularly update an inventory of its participants and third-party service providers and ensure that its cyber-resilience framework addresses its interconnections with those entities from a cyber-risk perspective.

(b) The SACCO's third-party risk assessment should be carried out regularly, considering the evolution of its threat landscape. It should, using a risk-based approach, ensure that the provision of outsourced services is commensurate with the cybersecurity posture of the vendor.

The SACCO should

(a) Assess third-party service provider's security capabilities at least through third- party self-assessment.

(b) Obtain assurance of the third-party service provider's cyber-resilience capabilities and may use tools such as certification, external audits (for example, SOC 2), summaries of test reports, service level agreements (SLAs) and key performance indicators.

(c) Ensure that there are appropriate procedures to isolate or block its third-party connections (in a timely manner) if there is a cyber-attack or a risk of contagion.

The independent audit function should validate an institution's third-party relationship management and outsourcing.

5.5.6. Cyber Threat Intelligence

The SACCO should

(d) Identify cyber threats that could materially affect its ability to perform or provide services as expected or that could have a significant impact on its ability to meet its own obligations or have knock-on effects within its ecosystem.

(e) Have capabilities in place to gather cyber-threat information from internal and external sources (for example, application, system and network logs; security products such as firewalls and IDSs; trusted threat-intelligence providers; and publicly available information sources).

(f) Belong or subscribe to a threat and vulnerability information-sharing source or ISAC that provides information on cyber threats and vulnerabilities. Cyber-threat information gathered by an institution should include analysis of tactics, techniques and procedures (TTPs) of real-life attackers, their modus operandi and information on geopolitical developments that may trigger cyber-attacks on any entity within an institution's ecosystem.

(g) Have the capabilities to analyses the cyber-threat information gathered from different sources, while taking into account its business and technical characteristics to

  (i) determine the motivation and capabilities of threat actors (including their TTPs) and the extent to which an institution is at risk of a targeted attack from them.

  (ii) assess the risk of technical vulnerabilities in operating systems, applications and other software, which could be exploited to perform attacks on the institution; and

  (iii) analyses cyber-security incidents experienced by other organisations (where available), including types of incidents and origin of attacks, the target of attacks, preceding threat events and frequency of occurrence, and determine the potential risk these pose to the institution.

The SACCO should analyze the cyber-threat intelligence to produce relevant cyber- threat intelligence and continuously use it to assess and manage security threats and vulnerabilities for the purpose of implementing appropriate cyber-security controls in its systems and, at a more general level, enhance its cyber-resilience framework and capabilities on a sustained basis.

5.5.7. Information Sharing

The SACCO should

(a) define the goals and objectives of information sharing in line with its business objectives and cyber resilience framework. At the very least, the objectives should include collecting and exchanging information in a timely manner that could facilitate the detection, response, resumption and recovery of its own systems and those of other sector participants during and following a cyber-attack.

(b) should define the scope of information-sharing activities by identifying the types of information available to be shared (for example, attackers' modus operandi, indicators of compromise, threats and vulnerabilities), the circumstances under which sharing this information is permitted (for example, in the case of a cyber incident), those with whom the information can and should be shared and how information provided to the institution and other sector participants will be acted upon.

(c) establish and implement protocols for sharing information relating to threats, vulnerabilities and cyber incidents with employees, having regard to their specific roles and responsibilities.

(d) have in place a process to access and share information with external stakeholders in a timely manner, such as regulators, law enforcement or other organisations within the institution's ecosystem.

(e) establish and regularly review information-sharing rules and agreements and implement procedures that allow information to be shared promptly and in line with the objectives and scope as delineated above, while, at the same time, meeting its obligations to protect potentially sensitive data that may have adverse consequences if disclosed improperly.

5.5.8. Incident Notification

a) In the event of a successful cyber-attack, SACCOS should notify Tanzania Cooperative Development Commission within two hours of verifying the incident. SACCOS should be ready to provide updates on the incident which the Tanzania Cooperative Development Commission may request. See incident notification form in Appendix A.

b) Once SACCOS is satisfied, that it has contained and recovered from an incident, it shall submit a report to the Tanzania Cooperative Development Commission. The report is expected at most on the fourth working days since the incident was detected. Should investigations not been complete, the report shall contain available information and a note that a full report shall be submitted at conclusions of investigations.

5.5.9. Comprehensive testing programme

SACCOS should establish a comprehensive testing programme to validate the effectiveness of its cyber resilience framework on a regular and frequent basis. It should employ appropriate cyber threat intelligence to inform its testing methods – for example, by designing tests to simulate advanced threat agent capabilities and extreme but plausible scenarios.

6. REMEDIAL MEASURES AND ADMINISTRATIVE SANCTIONS

Tanzania Cooperative Development Commission (TCDC) shall monitor SACCOS compliance with these Guidelines. The SACCOS fails to comply with these guidelines in a deliberate manner and which results or threatens to result in an unsafe or unsound operating condition as determined by Tanzania Cooperative Development Commission, such SACCOS shall be taken an administrative measure (any or all corrective actions and penalties) as provided for under regulation 85(h) & 85(i) of the Microfinance (Savings and Credit Cooperative Societies) regulations 2019.

7. APPENDIX

7.1 Appendix A: Cybersecurity Incident Reporting Form

CYBERSECURITY INCIDENT NOTIFICATION FORM TO TCDC			
Name of SACCOS: Registration number: License number: Mobile: Email:			
Date: (dd/mm/yy)		Time: (HH:MM)	
Cyber Incident Prioritization			Mark X
High	The incident affects the whole SACCOS. All or most of the SACCOS critical systems are affected		
Medium	The incident affects a section / division or multiple business units. It affects some part of the SACCOS operations		
Low	The incident affects an individual(s) and has little or no impact on the SACCOS operations		
Description of Cyber Incident			
Full Name of the Manager		Full Name of ICT officer	
Signature		Signature	