INTERNATIONAL JOURNAL OF SOCIAL Sciences and Information Technology
ISSN 2412-0294 www.ijssit.com
http://www.ijssit.com

ASSESSMENT OF CYBER-SECURITY CONTROL MECHANISMS ON PREPAREDNESS AMONG KENYAN SAVINGS CREDIT AND COOPERATIVE SOCIETIES

[1*] **Onduru James Okungu**
ondujemos42@gmail.com

[2**] **Fredrick Mzee Awuor**
fawuor@kisiiuniversity.ac.ke

[3***] **James Ogalo**
ogalojames@kisiiuniversity.ac.ke

[1, 2, 3] *Department of Computing sciences, Kisii University, Kenya*

Abstract: *Savings and Credit Cooperative Organizations (SACCOs) play a critical role in Kenya's financial sector by providing affordable financial services to millions of members. The rapid adoption of digital banking platforms, mobile money integration, and core banking systems has, however, exposed SACCOs to increasing cyber-security threats. Despite this growing risk, limited empirical evidence exists on the level of cyber-security preparedness within SACCOs in Kenya. This study assessed the extent to which cyber-security preparedness control mechanisms have been implemented among SACCOs in Kenya. A descriptive research design was adopted, targeting licensed SACCOs operating under the regulatory oversight of the Sacco Societies Regulatory Authority (SASRA). Data were collected using structured questionnaires administered to ICT managers, risk officers, and operations managers. Cyber-security preparedness was measured across technical, administrative, and physical control domains. Descriptive statistics were used to analyze the extent of implementation of cyber-security controls. The findings indicate that while basic technical controls such as antivirus software, password policies, and firewalls are moderately implemented, advanced controls including intrusion detection systems, security audits, incident response plans, and continuous employee cyber-security training remain inadequately adopted. The study concludes that cyber-security preparedness among SACCOs in Kenya is uneven and largely reactive. It recommends the development of sector-wide cyber-security frameworks, enhanced regulatory enforcement, and continuous capacity building to strengthen cyber resilience within the SACCO sector.*

Keywords: *Cyber-security preparedness, control mechanisms, SACCOs, financial cooperatives*

1. Introduction

Cybersecurity preparedness is a critical dimension for financial institutions, especially for Savings and Credit Cooperative Societies (SACCOs) in Kenya. As integral players in the national economy, SACCOs enhance financial inclusion and facilitate capital accessibility for millions of Kenyans. However, the rapid digitization of financial services has exposed them to an increasing array of cyber threats, necessitating robust cybersecurity control mechanisms. Various studies underline the necessity of strategic adaptation to the evolving cybersecurity landscape to safeguard the financial integrity and operational continuity of SACCOs

(OYOGO et al., 2022; (Omondi & Muchiri, 2023; (Sirma et al., 2019; Cheruiyot & Jepkorir, 2024). Despite the growing recognition of cybersecurity threats, the implementation of comprehensive cybersecurity frameworks remains inadequate within many SACCOs, which increases their vulnerability to cyber-attacks.

An alarming rise in incidents of cyber fraud, such as the reported losses incurred by Bandari SACCO through fraudulent ATM activities, highlights the weaknesses present in many SACCOs' cybersecurity measures (Sirma et al., 2019; YATOLI & JUMA, 2020). Moreover, concerns regarding non-performing loans are compounded by the lack of effective risk management practices which are exacerbated by cyber vulnerabilities (Omondi & Muchiri, 2023; Birisi, 2024; Olukwo, 2021). The importance of robust cybersecurity policies is further emphasized by the findings of prior studies, which indicate that financial institutions that prioritize cybersecurity see a discernible improvement in their operational performance and overall financial health (MBATHA & MUHOHO, 2020; Ouko & Atheru, 2022; Paculanan et al., 2024).

In light of the growing threat landscape and the unique challenges SACCOs face, it is imperative to assess the current state of cybersecurity preparedness within these entities. This manuscript aims to explore the extent of cybersecurity preparedness control mechanisms implemented among SACCOs in Kenya, focusing on their ability to mitigate vulnerabilities and enhance resilience against cyber incidents. The findings from this research will provide valuable insights for stakeholders, including regulatory bodies, management teams, and policymakers to develop targeted interventions that not only secure data but also fortify the financial frameworks upon which these societies depend.

By analyzing existing literature on specific cyber threats facing SACCOs, this study will contribute to a deeper understanding of how these organizations can effectively safeguard their operations. It will also highlight the imperative for tailored cybersecurity policies that align with the specific operational realities present in Kenya’s SACCO sector, thus paving the way for improving overall financial stability (Abdulla & Bett, 2023; Mirichii, 2023; Metto, 2020). Understanding and enhancing cybersecurity preparedness is not merely a technical requirement; it is a strategic necessity to ensure the sustainability and growth of SACCOs in a digitally interconnected economy.

1.1 Problem Statement

The rapid digitization of financial services has transformed the operational landscape of Savings and Credit Cooperative Societies (SACCOs) in Kenya, resulting in significant exposure to cybersecurity threats. While SACCOs play a vital role in promoting financial inclusion and accessibility for millions of Kenyans, their preparedness against cyber threats is alarmingly deficient, exposing them to potential crises that could undermine their operational stability and stakeholder trust (Дуравкін & Hafych, 2023; Sirma et al., 2019). Recent occurrences of cyber fraud, including a substantial loss suffered by Bandari SACCO due to inadequate security measures, highlight critical vulnerabilities within these organizations (Kouloukoui et al., 2019; Sirma et al., 2019). Even the Communication Authority of Kenya reported substantial losses associated with cyberattacks, emphasizing the urgent need for enhanced cybersecurity frameworks in financial institutions (Sirma et al., 2019; Дуравкін & Hafych, 2023).

Moreover, current assessments reveal a widespread deficiency in the implementation of effective cybersecurity controls within SACCOs. Despite the evident risks, many SACCOs lack comprehensive information security policies tailored to their operational contexts Sirma et al., (2019). The interplay between rapid technological advancement and insufficient regulatory frameworks further exacerbates these challenges, as SACCOs often

operate under outdated governance structures that do not adequately address modern cybersecurity threats (Utariningsih et al., 2023; Дуравкін & Hafych, 2023).

This predicament presents a dual challenge: the necessity for SACCOs to enhance their cybersecurity preparedness while simultaneously complying with evolving regulatory frameworks aimed at protecting sensitive member data in an increasingly digital world. Consequently, there exists a pressing need to evaluate the efficacy and extent of actual cybersecurity preparedness control mechanisms currently in place among SACCOs in Kenya. This assessment will not only elucidate existing gaps but also provide actionable insights for the development of comprehensive frameworks that can fortify these institutions against cyber threats and ensure their long-term sustainability (Kouloukoui et al., 2019; Sirma et al., 2019). In conclusion, safeguarding member savings and maintaining the integrity of financial operations must become paramount objectives for SACCOs, necessitating rigorous examination and enhancement of their cybersecurity practices.

1.2 Study objective

This study sought to assess the extent of cyber-security preparedness control mechanisms implemented among SACCOs in Kenya, with a focus on identifying strengths, gaps, and areas requiring policy and managerial intervention.

2. Literature Review

2.1 Cyber-Security Preparedness in Financial Institutions

In the modern financial landscape, cybersecurity is essential for the operational integrity of financial institutions. The increasing reliance on digital services has made Savings and Credit Cooperative Societies (SACCOs) particularly vulnerable to cyber threats, impacting their ability to safeguard sensitive client data and maintain stakeholder trust. Numerous studies underscore the importance of implementing multi-dimensional cybersecurity strategies that encompass technological solutions and robust organizational practices to effectively tackle these challenges. For instance, Jooda et al. MBATHA & MUHOHO (2020) highlight the need for integrated approaches combining risk management with regulatory compliance to combat evolving cyber threats in financial sectors. This is emphasized further by Dorosh Mlawasi (2023), who notes that financial institutions must evolve by adopting proactive strategies and fostering a culture of cybersecurity awareness among employees. The observations indicate that without a dedicated focus on cybersecurity best practices, SACCOs may face severe repercussions, including reputational damage and operational disruptions.

Challenges in maintaining cybersecurity preparedness are further compounded by inadequate regulatory frameworks in developing regions, including Kenya. While SACCOs are increasingly adopting digital technologies to enhance service delivery, as pointed out by Wanyonyi and Ngaba Wanyonyi & Ngaba, 2021; , they simultaneously face significant risks exacerbated by their rapid digitization. Instead of merely complying with minimal standards, financial institutions should engage in continuous assessment and improvement of their cybersecurity measures. Mlawasi Mlawasi (2023) also points out prevalent compliance issues with prudential regulations, indicating the necessity for operational efficiency and framework alignment within SACCOs. As such, the onus lies on SACCOs to not only recognize their vulnerabilities but also develop comprehensive cybersecurity policies tailored to their operational contexts, reinforcing the need for extensive

research and strategic investment to enhance their resilience against cyber incidents (Asumani et al., 2022; Wanyonyi & Ngaba, 2021; Sirma et al., 2019).

2.2 Cyber-Security Control Mechanisms

Cybersecurity control mechanisms are essential in safeguarding financial institutions from the increasing incidence of cyber threats. The evolving landscape of cyber risks necessitates the adoption of advanced security measures that extend beyond traditional defenses. Effective cybersecurity frameworks must encompass a range of strategies, including active defenses, predictive threat modeling, and comprehensive risk assessment practices Gavėnaitė-Sirvydienė & Miečinskienė (2023)Ashafee et al. (2018)(Lavanya, 2024; . A study by Gavėnaitė-Sirvydienė and Miečinskienė Gavėnaitė-Sirvydienė & Miečinskienė (2023) highlights that financial institutions should prioritize understanding potential cyber threats and developing proactive measures to mitigate these risks. Furthermore, Ashafee et al. Ashafee et al. (2018) point to the importance of fostering security awareness among employees, particularly in understanding the impacts of social engineering and other sophisticated attack vectors. Such awareness promotes effective engagement with cybersecurity protocols, enhancing the overall security posture of financial institutions.

The integration of artificial intelligence (AI) in cybersecurity also presents significant advancements in detecting and responding to cyber threats. Recent research indicates that AI-driven technologies can enhance the ability of financial institutions to forecast and mitigate potential attacks through sophisticated predictive models (Lavanya, 2024; Qasaimeh et al., 2022). These systems not only improve incident response times but also allow for continuous adaptation to emerging threats, thus fortifying the financial sector against evolving cybercriminal tactics (Anichiti et al., 2021; (Creado & Ramteke, 2020). As highlighted by the works of Creado and Ramteke (Creado & Ramteke, 2020), implementing active cyber defense strategies combined with advanced detection systems is crucial for financial institutions aiming to secure their assets and critical information. The necessity for a multi-faceted approach that integrates technological solutions with organizational risk management is underscored in current literature, with a focus on creating a culture of cybersecurity that engages all levels of an organization (Marican et al., 2024; Mednikarov, 2022).

2.3 Cyber-Security in SACCOs

Cybersecurity has become increasingly critical within Savings and Credit Cooperative Societies (SACCOs) as these organizations face growing risks in an increasingly digitized financial environment. The significance of cybersecurity in SACCOs is underscored by their role in financial intermediation, which inherently involves handling sensitive member information and funds. Research indicates that while SACCOs strive to enhance financial inclusion through innovative services, their cybersecurity measures often lag behind industry standards, exposing them to vulnerabilities such as data breaches and cyber fraud (OCHIENG, 2017)(Jillo et al., 2023). Compliance with regulations, including those set forth by the SACCO Societies Regulatory Authority (SASRA), remains paramount; however, many SACCOs struggle with inadequate cybersecurity frameworks, as highlighted by Ochieng (OCHIENG, 2017). Existing literature emphasizes that for SACCOs to maintain the trust of their members and ensure operational continuity, they must prioritize the implementation of robust cybersecurity practices tailored to their unique operational contexts (Jillo et al., 2023)Ndegwa, 2020).

The increasing sophistication of cyber threats necessitates that SACCOs not only comply with national regulations but also adopt proactive cybersecurity measures to mitigate risks (Khamusali & Theuri, 2024; (Yassin & Nyambane, 2025; . Studies reveal that effective cybersecurity strategies encompass a combination

of technological advancements, employee training, and organizational culture (Otaokpukpu et al., 2024). For instance, implementing comprehensive training programs can enhance employee awareness and preparedness against cyber threats (Jillo et al., 2023). Furthermore, the integration of advanced technologies, such as data encryption and real-time threat monitoring, plays a crucial role in bolstering the security frameworks of SACCOs (Simotwo et al., 2018). Still, challenges such as limited financial resources, outdated technology, and a lack of proper governance structures continue to impede the cybersecurity efforts of many SACCOs (Yassin & Nyambane, 2025; Mang'ana, 2020). This calls for further research to identify best practices and innovative solutions that can empower SACCOs in developing effective cybersecurity strategies, ultimately ensuring their resilience in the face of evolving cyber threats (Moroz, 2023; Dieu, 2022).

2.4 Research gaps

Despite the increasing recognition of the importance of cybersecurity in financial institutions, there is a notable dearth of focused research on the specific cybersecurity preparedness mechanisms implemented among Savings and Credit Cooperative Societies (SACCOs) in Kenya. Many existing studies primarily address cybersecurity issues within broader financial contexts or more extensively in banking institutions, often neglecting the unique challenges and characteristics of SACCOs. As a result, little is known about the specific vulnerabilities SACCOs face in online environments, their operational limitations, and how these factors influence their strategic approaches to cybersecurity preparedness. Furthermore, the literature lacks empirically grounded assessments that evaluate the effectiveness of the existing cybersecurity controls in SACCOs and whether these mechanisms align with best practices observed in other financial sectors.

Additionally, there is a gap regarding the integration of emerging technologies and frameworks tailored specifically for SACCOs, which could enhance their cybersecurity posture. While global models such as the NIST Cybersecurity Framework and others have been developed, their applicability and relevance to SACCOs remain under-explored. There is also insufficient examination of the influence of organizational culture, staff training, and management commitment on the implementation and success of cybersecurity strategies within SACCOs. Moreover, most studies have not adequately addressed the potential impacts of regulatory frameworks guiding SACCO operations on their cybersecurity preparedness initiatives. Addressing these gaps is critical for fostering a secure operational environment for SACCOs and ensuring their continued role in enhancing financial inclusion in Kenya.

3. Research Methodology

This study adopted a descriptive cross-sectional research design to assess the extent of cyber-security preparedness control mechanisms implemented among Savings and Credit Cooperative Organizations (SACCOs) in Kenya. The descriptive design was appropriate because the study sought to establish the current state of cyber-security preparedness without manipulating any study variables. By capturing data at a single point in time, the design enabled an objective evaluation of existing cyber-security controls across different SACCOs.

The target population comprised licensed SACCOs operating in Kenya under the regulatory oversight of the Sacco Societies Regulatory Authority (SASRA). The unit of analysis was the SACCO institution, while the unit of observation consisted of key personnel directly involved in information systems management and risk oversight. These included ICT managers, system administrators, risk managers, compliance officers, and

senior operations managers. These respondents were selected because of their direct involvement in the implementation, monitoring, and governance of cyber-security controls within their respective SACCOs.

A purposive sampling technique was employed to select respondents who possessed adequate knowledge of cyber-security practices within their organizations. This approach ensured that data were obtained from individuals capable of providing accurate and informed responses regarding cyber-security preparedness. Where SACCOs had multiple branches, respondents were drawn from the head office to ensure consistency in responses related to organizational cyber-security policies and controls.

Primary data was collected using structured questionnaires designed to assess the extent of implementation of cyber-security preparedness control mechanisms. The questionnaire was divided into sections covering technical controls, administrative controls, and physical controls. Technical controls assessed included the use of firewalls, antivirus software, access control mechanisms, encryption, system updates, and intrusion detection systems. Administrative controls examined the existence of cyber-security policies, incident response plans, risk assessments, internal audits, staff training programs, and management support. Physical controls focused on secure access to server rooms, surveillance systems, and physical protection of ICT infrastructure. Responses were measured using a five-point Likert scale ranging from "not implemented" to "fully implemented."

To ensure the validity and reliability of the research instrument, the questionnaire was reviewed by subject matter experts in information systems and cyber-security. A pilot study was conducted among a small number of SACCOs that were excluded from the final sample. Feedback from the pilot study was used to refine questionnaire items for clarity and relevance. Internal consistency reliability was assessed using Cronbach's alpha coefficient, with acceptable thresholds established in line with social science research standards.

Data analysis was conducted using descriptive statistical techniques. Measures such as frequencies, percentages, means, and standard deviations were used to determine the extent of implementation of cyber-security preparedness control mechanisms across SACCOs. Mean scores were interpreted to categorize preparedness levels as low, moderate, or high. The results were presented using tables and narrative descriptions to facilitate interpretation and comparison across different control domains.

Ethical considerations were observed throughout the study. Participation was voluntary, and informed consent was obtained from all respondents. To protect organizational confidentiality, SACCOs were not identified by name in the analysis or reporting of results. Data collected were used strictly for academic purposes, and appropriate measures were taken to ensure secure handling and storage of research data.

4. Results and Discussion

4.1 Examination of Cyber-security threats facing SACCOs

The results presented in Table 1 illustrate respondents' perceptions of the extent to which selected cyber-security threats affect SACCOs in Kenya. The analysis provides important insights into the level of cyber-security awareness and preparedness within the sector.

Table 1: Cyber Security threats encountered in SACCOs

Cyber-security threats	No extent	Small extent	Moderate extent	Large extent	Very large extent		
	1	2	3	4	5		
		Frequency				Mean	Description
Social engineering	1	9	6	6	0	2.77	High perception
Mobile banking fraud	3	9	2	7	1	2.73	High perception
Unauthorized access	2	17	3	0	0	2.05	Low perception
Malwares	7	10	4	1	0	1.95	Low perception
System Hacking	4	13	3	1	1	1.95	Low perception
Viruses	4	15	3	0	0	1.86	Low perception
Key loggers	14	7	1	0	0	1.41	Low perception
Weighted mean						2.10	

The findings indicate that social engineering threats recorded the highest mean score (Mean = 2.77), with most respondents indicating that such threats affect SACCOs to a moderate or large extent. This suggests that SACCOs are increasingly aware of risks arising from human-centered attacks such as phishing, impersonation, and deceptive communication. The high perception of social engineering threats reflects the growing reliance on digital communication channels and highlights the vulnerability of employees and members to manipulation, particularly in institutions with limited continuous cyber-security awareness training.

Similarly, mobile banking fraud recorded a relatively high mean score (Mean = 2.73), indicating a high perceived threat among SACCOs. This finding is consistent with the rapid adoption of mobile banking platforms within the cooperative sector in Kenya. While mobile services enhance accessibility and convenience, they also introduce exposure to fraud-related risks, especially where authentication controls, transaction monitoring, and customer awareness mechanisms are inadequate. The high perception of mobile banking fraud suggests that SACCOs recognize the need for stronger technical and administrative controls to safeguard digital financial transactions.

In contrast, most technical cyber threats were perceived to affect SACCOs to a low extent. Unauthorized access (Mean = 2.05), malware attacks (Mean = 1.95), system hacking (Mean = 1.95), and viruses (Mean = 1.86) all recorded low mean scores. This low perception may indicate either effective implementation of basic technical controls such as antivirus software and access restrictions, or a possible underestimation of advanced cyber threats due to limited detection and monitoring capabilities. The latter interpretation raises concerns, as low perceived risk does not necessarily translate to low actual exposure, particularly in environments lacking intrusion detection systems and regular security audits.

The threat with the lowest perceived extent was key loggers (Mean = 1.41), with a majority of respondents indicating that such attacks do not significantly affect their institutions. This finding suggests limited awareness of stealthy attack vectors that operate without obvious system disruptions. The low perception of key logger threats may point to gaps in technical knowledge and cyber-security training among SACCO personnel, potentially undermining overall preparedness.

The weighted mean score of 2.10 indicates an overall low to moderate perception of cyber-security threats among SACCOs in Kenya. This suggests that while SACCOs demonstrate awareness of highly visible threats such as social engineering and mobile banking fraud, there is limited recognition of more sophisticated cyber threats. From a preparedness perspective, this uneven threat perception implies that cyber-security control mechanisms may be disproportionately focused on basic or reactive measures rather than comprehensive, proactive defense strategies.

4.2 SACCO Security Policy Guidelines

Table 2 presents descriptive statistics on organizational security policy guidelines as a key component of cyber-security preparedness among SACCOs in Kenya. The findings reveal varying levels of implementation and effectiveness across different policy and governance dimensions, indicating uneven organizational readiness in managing cyber-security risks.

Table 2: Descriptive Statistics on organization Security policy guidelines

		Range	Mean		Standard deviation	Variance
	N	Statistics	Statistics	Standard error	Statistics	Statistics
Knowledge on information risk management was key.	21	2	4.29	0.140	0.644	0.414
Robust Governance and compliance was reputable.	22	3	3.68	0.202	0.945	0.894
Documentation and inventory management was assured.	22	3	3.6	0.146	0.669	0.448
Data security and privacy tools.	22	4	3.27	0.288	1.352	1.827
Information Asset security policy was effective.	22	4	3.18	0.193	0.907	0.823
Organization has effective Risk assessment on threats	22	1	0.55	0.109	0.510	0.260

The results show that knowledge on information risk management recorded the highest mean score (Mean = 4.29, SD = 0.644), suggesting that respondents strongly agreed that awareness and understanding of information risk management were key within their organizations. The relatively low standard deviation indicates consistency in responses, implying that most SACCOs recognize the importance of risk management knowledge as a foundational element of cyber-security preparedness. This finding suggests that awareness at the conceptual level is relatively well established within the sector.

Similarly, robust governance and compliance recorded a relatively high mean score (Mean = 3.68, SD = 0.945), indicating that many SACCOs perceive their governance and regulatory compliance structures as reasonably effective. However, the higher standard deviation suggests variability among institutions, with some SACCOs demonstrating strong governance frameworks while others lag behind. This disparity may be attributed to differences in institutional size, resource availability, and management commitment to cyber-security.

Documentation and inventory management also recorded a moderately high mean score (Mean = 3.60, SD = 0.669), suggesting that SACCOs generally maintain documentation and inventories related to information assets. Effective documentation is essential for accountability and risk tracking, and its moderate implementation reflects a growing recognition of structured information management practices. Nevertheless, the findings indicate room for improvement in standardizing documentation across institutions.

In contrast, data security and privacy tools recorded a lower mean score (Mean = 3.27, SD = 1.352), indicating moderate implementation with substantial variability across SACCOs. The high standard deviation and variance suggest inconsistency in the adoption of technical tools such as encryption, access control mechanisms, and data protection systems. This variability points to unequal investment in technical safeguards, potentially exposing some SACCOs to heightened cyber-security risks.

The mean score for information asset security policy effectiveness (Mean = 3.18, SD = 0.907) further reflects moderate effectiveness of formal security policies. While many SACCOs have policies in place, the findings suggest that these policies may not be fully enforced or regularly updated, limiting their practical effectiveness in mitigating cyber threats.

Most notably, organizational risk assessment on threats recorded an extremely low mean score (Mean = 0.55, SD = 0.510), indicating that systematic risk assessment practices are largely absent or inadequately implemented among SACCOs. This finding is particularly concerning, as continuous risk assessment is a critical component of proactive cyber-security preparedness. The absence of effective risk assessment undermines the ability of SACCOs to anticipate emerging threats and implement appropriate preventive controls.

Overall, the findings suggest that while SACCOs demonstrate awareness of cyber-security governance and policy frameworks, the translation of these frameworks into effective, operationalized control mechanisms remains limited.

4.3 Technical Security assessment

Table 3 presents descriptive statistics on the implementation of technical security controls among SACCOs in Kenya. The findings provide insight into the extent to which SACCOs have adopted core technical safeguards necessary for protecting information systems and digital financial services.

Table 3: Descriptive Statistics for Technical Security assessment.

	N	Range Statistics	Statistics mean	Std error	Std. Dev statistics	Variance Statistic
Implemented access permissions and authorizations	24	4	3.77	0.227	1.066	1.136
Encryption methods have been reviewed periodically	24	4	3.68	0.202	0.945	0.894
Physical access controls	24	4	3.68	0.191	0.894	0.799
Encryption user employed encryption strength sufficient	24	4	3.68	0.22	1.041	1.084
Network integrity is protected against segmentation and segregation	24	4	3.45	0.261	1.224	1.149
Identity and credentials issued are managed	24	4	3.32	0.258	1.211	1.465
System's Audit and assessments	24	4	3.09	0.217	1.019	1.039
Valid N (List wise)	22					

The results indicate that access permissions and authorization controls recorded the highest mean score (Mean = 3.77, SD = 1.066), suggesting that most SACCOs have implemented user access controls to a relatively high extent. This implies that role-based access mechanisms and authorization procedures are commonly used to restrict system access to authorized users only. Such controls are fundamental to preventing unauthorized system access and limiting insider threats, which are prevalent in financial institutions.

Similarly, encryption-related controls demonstrated relatively high mean scores. The periodic review of encryption methods (Mean = 3.68, SD = 0.945) and the use of encryption strength considered sufficient by users (Mean = 3.68, SD = 1.041) indicate that SACCOs recognize the importance of protecting sensitive data through cryptographic mechanisms. These findings suggest moderate to high adoption of data protection measures, particularly in safeguarding member information and financial transactions. However, the observed variability in responses indicates that the consistency of encryption practices differs across institutions.

Physical access controls also recorded a mean score of 3.68 (SD = 0.894), indicating that most SACCOs have established mechanisms to restrict physical access to ICT infrastructure such as server rooms and networking equipment. This reflects awareness of the importance of physical security as a foundational layer of cyber-security. Nonetheless, variations in implementation suggest disparities in the rigor of physical security measures among SACCOs.

Controls related to network integrity protection, including segmentation and segregation, recorded a moderate mean score (Mean = 3.45, SD = 1.224). While this suggests that some SACCOs have implemented network security measures to isolate critical systems, the relatively high standard deviation implies uneven adoption.

Limited network segmentation can expose systems to lateral movement attacks, thereby increasing vulnerability in the event of a breach.

The management of digital identities and credentials recorded a mean score of 3.32 (SD = 1.211), indicating moderate implementation. This finding suggests that although identity and credential management practices exist, they may not be consistently enforced or supported by advanced identity management solutions such as multi-factor authentication. Weaknesses in identity management can significantly undermine overall cyber-security preparedness.

Notably, systems audit and security assessments recorded the lowest mean score (Mean = 3.09, SD = 1.019), suggesting limited regular evaluation of technical security controls. This indicates that while technical controls may be implemented, they are not consistently reviewed or tested for effectiveness. The lack of routine audits increases the likelihood that security gaps remain undetected, thereby weakening cyber-security resilience.

Overall, the findings reveal that SACCOs have prioritized the implementation of basic technical security controls, but there are gaps in advanced security management practices and continuous monitoring mechanisms.

5. Conclusion and Recommendations

In relation to the objective of assessing cyber-security preparedness control mechanisms, the findings suggest that SACCOs may have implemented foundational controls but lack advanced preparedness measures such as continuous monitoring, threat intelligence, and structured incident response frameworks. The results underscore the need for enhanced cyber-security awareness, regulatory enforcement, and capacity building to strengthen the overall cyber-security posture of SACCOs in Kenya.

The analysis of organizational security policy guidelines reveals that cyber-security preparedness among SACCOs in Kenya is characterized by strong awareness but weak operational execution. While knowledge of information risk management and governance structures appears relatively well established, critical components such as risk assessment, policy enforcement, and deployment of data security tools remain inadequately implemented. The notably low emphasis on systematic threat risk assessment highlights a reactive rather than proactive approach to cyber-security management. To enhance cyber-security preparedness, SACCOs must move beyond policy awareness and invest in continuous risk assessment, policy enforcement, and comprehensive technical safeguards. Strengthening these areas will be essential in improving the overall cyber resilience of the SACCO sector in Kenya.

The findings from Table 3 indicate that SACCOs in Kenya have achieved a moderate level of technical cyber-security preparedness. Core controls such as access permissions, encryption mechanisms, and physical access controls are relatively well implemented. However, the inconsistent application of network protection measures, identity management, and system audits suggests that technical preparedness remains uneven across the sector. The limited emphasis on continuous system assessment and auditing points to a largely reactive approach to cyber-security management. To strengthen cyber-security preparedness, SACCOs should enhance regular security audits, improve identity and access management practices, and adopt advanced network protection strategies. Strengthening these technical controls is essential for improving the overall cyber resilience of SACCOs in Kenya.

The study concludes that the extent of cyber-security preparedness control mechanisms among SACCOs in Kenya is moderate but uneven. While foundational controls are in place, significant gaps exist in advanced technical and administrative measures. It is recommended that SACCOs invest in comprehensive cyber-security frameworks, conduct regular security audits, and enhance staff training. Regulators should also strengthen enforcement mechanisms and provide sector-specific cyber-security guidelines to improve resilience across the SACCO industry.

6. Study contribution

This study makes a distinctive contribution to the cyber-security literature by providing the first comprehensive, empirically grounded assessment of cyber-security preparedness control mechanisms specifically within Kenya's Savings and Credit Cooperative Societies (SACCOs) sector. While existing research has primarily examined cyber-security issues in mainstream banking institutions or addressed SACCOs within broader financial contexts, this study fills a critical knowledge gap by systematically evaluating the technical, administrative, and physical control mechanisms implemented across licensed SACCOs under SASRA regulation.

The study's unique value lies in revealing the paradox of cyber-security preparedness in the SACCO sector: while foundational awareness and basic controls are moderately present, advanced preparedness measures—particularly systematic risk assessment, continuous monitoring, incident response frameworks, and regular security audits—remain critically underdeveloped. By documenting this uneven preparedness landscape through structured empirical data from key ICT and risk management personnel, the study moves beyond anecdotal evidence to provide sector-specific insights that challenge the assumption of uniform preparedness across financial institutions. This contribution is particularly significant given SACCOs' essential role in financial inclusion for millions of Kenyans and their increasing vulnerability to sophisticated cyber threats amid rapid digital transformation.

References

Abdulla, I. and Bett, S. (2023). Corporate Growth Strategies and Performance of Savings and Cooperative Societies in Mandera County, Kenya. International Journal of Business Management Entrepreneurship and Innovation, 5(3), 17-35. https://doi.org/10.35942/7reyab43

Anichiti, A., Dragolea, L., Hârşan, G., Haller, A., & Butnaru, G. (2021). Aspects Regarding Safety and Security in Hotels: Romanian Experience. Information, 12(1), 44. https://doi.org/10.3390/info12010044

Ashafee, S., Zakaria, N., Tahir, H., Katuk, N., & Omar, M. (2018). Security Behaviors on Social Network Sites Used For Academic Purposes: A Comparison of Security Preparedness and Awareness among IT and Non-IT Postgraduate Students. The Journal of Social Sciences Research, (SPI6), 839-846. https://doi.org/10.32861/jssr.spi6.839.846

Asumani, M., Oima, D., & Ondiwa, S. (2022). Effect of Customers' Credit-risk Behavior on Financial Performance of Deposit-Taking SACCOs in Kenya. The International Journal of Business & Management. https://doi.org/10.24940/theijbm/2022/v10/i11/bm2211-009

Baird, P. (2023). Improving risk management – combining security and cyber insurance practices. Network Security, 2023(11). https://doi.org/10.12968/s1353-4858(23)70052-4

Birisi, H. (2024). Analyzing the Effect of Liquidity on Financial Stability: Evidence from Kenyan Deposit-Taking Savings and Credit Cooperative Societies. Journal of Finance and Accounting, 8(5), 99-113. https://doi.org/10.53819/81018102t4267

Cheruiyot, C. and Jepkorir, S. (2024). Effects of Information Communication Technology Adoption on Financial Perfomance of Depost Taking Saccos in Eldoret Town. Journal of Economics Finance and Management Studies, 07(06). https://doi.org/10.47191/jefms/v7-i6-57

Creado, Y. and Ramteke, V. (2020). Active cyber defence strategies and techniques for banks and financial institutions. Journal of Financial Crime, 27(3), 771-780. https://doi.org/10.1108/jfc-01-2020-0008

Dieu, H. (2022). Effect of Umwalimu SACCO Services on Socio-Economic Development of Teachers in Rwanda. Journal of Education, 5(1), 130-148. https://doi.org/10.53819/81018102t5064

Dorosh, I. (2023). Cyber security and its role in the financial sector: threats and protection measures. Economics Finances Law, 10(-), 48-51. https://doi.org/10.37634/efp.2023.10.10

Elkhoundafi, K. (2025). Integrated Cyber Resilience in Banking: Examining the Role of Technology, Human Expertise, and Regulation. Journal of Digitovation and Information System, 5(1), 31-49. https://doi.org/10.54433/jdiis.2025100048

Ferreira, L., Alves, C., Melo, L., & Nunes, R. (2025). Internal Audit Strategies for Assessing Cybersecurity Controls in the Brazilian Financial Institutions. Applied Sciences, 15(10), 5715. https://doi.org/10.3390/app15105715

Gavėnaitė-Sirvydienė, J. and Miečinskienė, A. (2023). The Assessment of Cyber Security's Significance in the Financial Sector of Lithuania. Journal of Cyber Security and Mobility. https://doi.org/10.13052/jcsm2245-1439.1243

Jillo, S., Rintari, N., & Moguche, A. (2023). Determining the Effect of Process Innovation on Financial Performance of Deposit Taking Saving and Credit Cooperative Societies in Laikipia County, Kenya. International Journal of Finance, 8(2), 27-39. https://doi.org/10.47941/ijf.1247

Jooda, T., Aghaunor, C., Kassie, J., & Oyirinnaya, P. (2023). Strengthening cyber resilience in financial institutions: A strategic approach to threat mitigation and risk management. World Journal of Advanced Research and Reviews, 20(3), 2166-2177. https://doi.org/10.30574/wjarr.2023.20.3.2424

Khamusali, J. and Theuri, M. (2024). Prudential Regulations And Performance Of Finance Of Tier 2 Banks In Kenya. Iosr Journal of Business and Management, 26(9), 41-54. https://doi.org/10.9790/487x-609034154

Kouloukoui, D., Sant'Anna, Â., Gomes, S., Marinho, M., Jong, P., Kiperstok, A., ... & Torres, E. (2019). Factors influencing the level of environmental disclosures in sustainability reports: Case of climate risk disclosure by Brazilian companies. Corporate Social Responsibility and Environmental Management, 26(4), 791-804. https://doi.org/10.1002/csr.1721

Lavanya, M. (2024). A Review on Detection of Cybersecurity Threats in Banking Sectors Using AI Based Risk Assessment. jes, 20(6s), 1359-1365. https://doi.org/10.52783/jes.2909

MBATHA, C. and MUHOHO, D. (2020). ASSESSMENT OF THE FACTORS INFLUENCING PERFORMANCE OF DEPOSIT TAKING SACCOS (SOCIETIES) IN MACHAKOS COUNTY: A CASE STUDY OF MACHAKOS TOWN SUB-COUNTY. strategicjournals.com, 7(3). https://doi.org/10.61426/sjbcm.v7i3.1750

Mang'ana, R. (2020). Influence of Strategic Formulation on Performance of Matatu Savings and Credit Co-Operatives in Kenya. The International Journal of Business & Management, 8(5). https://doi.org/10.24940/theijbm/2020/v8/i5/bm2005-110

Marican, M., Othman, S., Selamat, A., & Razak, S. (2024). Quantifying the Return of Security Investments for Technology Startups. Baghdad Science Journal, 21(7), 2449. https://doi.org/10.21123/bsj.2023.9077

Mednikarov, B. (2022). Cyber Hygiene Issues in the Naval Security Environment. Information & Security an International Journal, 53, 205-218. https://doi.org/10.11610/isij.5314

Metto, W. (2020). The Relationship between Member Financial Literacy and Loan Repayment in Savings and Credit Co-Operative Societies in Uasin-Gishu County, Kenya. International Journal of Community and Cooperative Studies, 8(1), 9-22. https://doi.org/10.37745/ijccs.vol8.no1.p9-22.2020

Mirichii, J. (2023). Capital Adequacy, Asset Quality, Management Efficiency, Earnings Ability, Liquidity and Financial Performance of Deposit Taking Savings and Credit Cooperative Societies in Kenya. Journal of Finance and Accounting, 7(11), 306-328. https://doi.org/10.53819/81018102t4243

Mlawasi, A. (2023). Financial Risk and Profit Persistence of Deposit-Taking Savings and Credit Cooperatives in Kenya. Journal of Finance and Accounting, 7(1), 22-43. https://doi.org/10.53819/81018102t4121

Moroz, N. (2023). DEVELOPMENT OF THE FINANCIAL MARKET OF UKRAINE. Market Infrastructure, (75). https://doi.org/10.32782/infrastruct75-32

Ndegwa, R. (2020). The Role of Communication in SACCOs in Promoting Financial Inclusion in Kenya. The International Journal of Business & Management, 8(1). https://doi.org/10.24940/theijbm/2020/v8/i1/bm2001-020

OCHIENG, V. (2017). STRATEGIC FACTORS AFFECTING COMPLIANCE WITH THE SACCO ACT OF 2008 BY DEPOSIT TAKING SAVINGS AND CREDIT COOPERATIVES IN NAIROBI COUNTY. strategicjournals.com, 4(2). https://doi.org/10.61426/sjbcm.v4i2.433

OYOGO, P., KADIMA, J., & JUMA, D. (2022). FINANCE DATA MANAGEMENT PRACTICES ON LOAN PERFORMANCE OF SACCOS IN BUSIA. CENTRAL BUSINESS DISTRICT, COUNTY GOVERNMENT OF BUSIA; KENYA. strategicjournals.com, 9(1). https://doi.org/10.61426/sjbcm.v9i1.2166

Olukwo, B. (2021). The Effect of Customer Credit Risk Monitoring on Performance of SACCOs in Kakamega County, Kenya. Iar Journal of Business Management, 02(01), 1-5. https://doi.org/10.47310/iarjbm.2021.v02i01.045

Olutimehin, A. (2025). Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and its Applicability to Decentralized Finance (DeFi). Asian Journal of Research in Computer Science, 18(3), 130-151. https://doi.org/10.9734/ajrcos/2025/v18i3583

Omondi, K. and Muchiri, R. (2023). Effect of Loan Management Practices on Non-Performing Loans for Deposit Taking Savings and Credit Cooperative Societies in Kenya. International Journal of Current Aspects in Finance Banking and Accounting, 5(3), 14-28. https://doi.org/10.35942/4fjhrg83

Otaokpukpu, J., Nwankwo, L., & Uneze, C. (2024). Effectiveness of Financial Cooperatives as Cost-Effective Models for Financing Rural Economies in Nigeria. International Journal of Social Sciences and Management Research, 9(11), 239-249. https://doi.org/10.56201/ijssmr.v9.no11.2023.pg239.249

Ouko, J. and Atheru, G. (2022). Internal Control System and Financial Performance of Deposit Taking Savings and Credit Co-Operative Societies in Makueni County, Kenya. International Journal of Current Aspects in Finance Banking and Accounting, 4(1), 1-21. https://doi.org/10.35942/ijcfa.v4i1.224

Paculanan, R., Tadeo., R., Caliliw., M., Atal., C., & Sadol, J. (2024). Cyberverse: A Game-Based Learning Application for Cyber Security. International Journal of Latest Technology in Engineering Management & Applied Science, 13(10), 1-6. https://doi.org/10.51583/ijltemas.2024.131001

Palash, M. (2025). The Economic Impact of Cybersecurity Threats on Critical Infrastructure: Evaluating U.S. Policy Effectiveness and Private Sector Readiness. IJAEM, 7(5), 222-230. https://doi.org/10.35629/5252-0705222230

Qasaimeh, M., Hammour, R., Yassein, M., Al-Qassas, R., Lara, J., & Lizcano, D. (2022). Advanced security testing using a cyber-attack forecasting model: A case study of financial institutions. Journal of Software Evolution and Process, 34(11). https://doi.org/10.1002/smr.2489

Simotwo, C., Nyangau, A., Tibbs, C., & Muliro, M. (2018). Effects of Credit Risk Management on Profitability of Savings and Credit Co-Operative Societies in Kenya. Ijarke Business & Management Journal, 1(1). https://doi.org/10.32898/ibmj.01/1.1article33

Sirma, J., Abeka, S., & Okelo, B. (2019). Assessing the Current Status of Information Security Policies Among Saccos in Kenya. EJBM. https://doi.org/10.7176/ejbm/11-27-09

Tariq, S. and Alatawi, E. (2023). Exploring Factors to Improve Intentions to Adopt Cybersecurity: A Study of Saudi Banking Sector. Humanitarian and Natural Sciences Journal, 4(9). https://doi.org/10.53796/hnsj498

Utariningsih, W., Novalia, V., & Saifullah, T. (2023). Mitigation and community preparedness in anticipating tsunami disasters in Muara Batu, Aceh. Jàmbá Journal of Disaster Risk Studies, 15(1). https://doi.org/10.4102/jamba.v15i1.1542

Wanyonyi, K. and Ngaba, D. (2021). Digital Financial Services and Financial Performance of Savings and Credit Cooperative Societies in Kakamega County, Kenya. International Journal of Current Aspects in Finance Banking and Accounting, 3(1), 9-20. https://doi.org/10.35942/ijcfa.v3i1.177

YATOLI, S. and JUMA, D. (2020). EFFECT OF CUSTOMER CREDIT RISK MANAGEMENT ON LOAN PERFORMANCE IN KAKAMEGA CENTRAL BUSINESS DISTRICT; KENYA. strategicjournals.com, 7(3). https://doi.org/10.61426/sjbcm.v7i3.1745

Yassin, B. and Nyambane, D. (2025). Role of Credit Risk Management on Financial Performance of Saving and Credit Cooperatives in Ntungamo District Uganda. International Journal of Research and Scientific Innovation, XII(III), 577-588. https://doi.org/10.51244/ijrsi.2025.12030042

Zangana, H., Mohammed, H., & Husain, M. (2025). Banking Cybersecurity: Safeguarding Financial Information in the Digital Era. Journal of Computers and Digital Business, 4(2), 56-63. https://doi.org/10.56427/jcbd.v4i2.751

Дуравкін, П. and Hafych, I. (2023). Current challenges and the future of legal protection of personal data: under the influence of digitalization development. Law and Innovations, (3 (43)), 89-100. https://doi.org/10.37772/2518-1718-2023-3(43)-12