Open Access Library Journal
2024, Volume 11, e10810
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Cybersecurity Framework for Kenyan Universities in Conformity with ISO/IEC 27001:2022 Standard

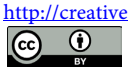
Patrick Macharia Gichubi, Bernard Maake, Ruth Chweya

Department of Computing and Informatics, School of Information Science and Technology, Kisii University, Kisii, Kenya
Email: pmgichubi@gmail.com, bmaake@kisiiuniversity.ac.ke, rchweya@kisiiuniversity.ac.ke

How to cite this paper: Gichubi, P., Maake, B. and Chweya, R. (2024) Cybersecurity Framework for Kenyan Universities in Conformity with ISO/IEC 27001:2022 Standard. *Open Access Library Journal*, **11**: e10810.
https://doi.org/10.4236/oalib.1110810

Received: September 25, 2023
Accepted: August 27, 2024
Published: August 30, 2024

Copyright © 2024 by author(s) and Open Access Library Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/



Open Access

Abstract

The rapid adoption of enterprise resource planning (ERP), the necessity for remote access to information systems, and the swift development of digital technologies like IoT and cloud computing have increased cyberattacks on organizations, including universities. Despite not being as heavily targeted as major industries, universities have become more vulnerable due to open ERP systems, insufficient cybersecurity investment, and limited cyber expertise. This study aimed to enhance cybersecurity in Kenyan universities by identifying cybersecurity threats, assessing existing controls, and proposing a cybersecurity framework aligned with the ISO/IEC 27001:2022 standard. A descriptive survey method was used to gather quantitative data, employing Design Science Research Methodology (DSRM) for Information Systems research. The target population comprised 60 chartered Kenyan universities, divided into public and private categories. Purposive sampling selected respondents from each sampled university, while simple random sampling chose universities from each cluster. Out of 48 questionnaires distributed via Google Forms, 45 were returned, yielding a 93.75% response rate. Statistical tools such as frequency, percentages, mean, and standard deviation were used for data analysis, with results presented in tables and figures. Findings revealed that most universities had experienced cyberattacks and faced significant cybersecurity threats. Furthermore, many universities lacked adequate cybersecurity policies and controls, including organizational, human, physical, and technological measures. The proposed cybersecurity framework was evaluated and deemed suitable for mitigating cybersecurity risks in Kenyan universities. The study recommended conducting comparative studies between Kenyan universities and institutions in other countries to identify and adapt best practices to the Kenyan context.

Subject Areas

Cybersecurity, Information Security, ISO/IEC 27001, Cybersecurity Frameworks

Keywords

Cybersecurity, ISO/IEC 27001, Standards, Framework, Threats, Risks, Kenya, University

1. Introduction

This study addresses rising cybersecurity threats in Kenyan universities by proposing a tailored framework aligned with ISO/IEC 27001:2022 standard. Kenyan universities, holding sensitive data, are prime targets for cyberattacks. The framework aims to bolster cybersecurity preparedness and offers a model for global educational institutions. With global cybercrime on the rise, this proactive approach is vital. The study focuses on chartered Kenyan universities and ICT personnel, potentially influencing future cybersecurity framework research.

1.1. Background of the Study

The growing adoption of enterprise resource planning (ERP) systems, increased reliance on remote access to information systems, and the rapid expansion of digital and cloud technologies have made organizations more susceptible to cyberattacks. [1] conducted a 2022 survey, revealing that 64% of firms experienced ERP data breaches since 2020, resulting in unforeseen downtime, heightened compliance risks, damaged corporate reputations, financial losses, and project delays [1]. A report by Momentum Cyber in 2020 found that ransomware attacks occur approximately every eleven seconds, costing an average of $1.8 million for recovery, with 43% of breaches affecting small and medium-sized enterprises (DeWalt & McAlpine, 2020). Furthermore, a 2022 study by Checkpoint Software Technologies highlighted that the education and research sectors are prime targets, accounting for 75% of cyberattacks due to their continued reliance on outdated practices and frameworks ill-suited for evolving threats [2]. In academia, cybersecurity threats have surged, primarily because services are now delivered through ERP systems [3]. [4] observed that while academic institutions may not be as prominent targets as major industries, their open and transparent ERP infrastructure, insufficient security measures during system procurement, and limited cybersecurity expertise have made them appealing targets. To address these challenges and bolster cybersecurity, universities are considering the adoption of international cybersecurity standards, guidelines, and frameworks. Given this context, establishing a dedicated cybersecurity framework for Kenyan universities is imperative to mitigate the evolving cyber risks they face.

1.2. Statement of the Problem

Universities face escalating cybersecurity threats due to the abundance of sensitive data they store, including student information and intellectual property [5]. The education and research sectors are prime targets, witnessing a 75% increase in attacks in 2022, averaging 1605 attacks per organization per week [3]. Cyberattacks on universities are relentless, focusing on infiltrating ERP databases and ransom attacks [6]. Kenya is also grappling with a surge in cyberattacks, impacting critical government platforms and academic institutions [7]. Incidents in universities have been on the rise, often unreported, with students increasingly involved in cyberattacks [7]. Lawsuits have emerged over student suspensions tied to cyberattacks on examinations [8]. Universities face breaches compromising student and staff data [9].

Cyberattacks extend to tampering with academic records and financial data, even targeting internet connectivity for illicit gains [9] [10]. Ransomware attacks have also plagued universities, demanding substantial sums and threatening severe consequences [7] [11]. Given this alarming landscape, this study aims to address the pressing need for improved cybersecurity in Kenyan universities by proposing a cybersecurity framework aligned with ISO/IEC 27001:2022 standard [11]. The framework seeks to protect sensitive data, mitigate cyber threats, and enhance overall cybersecurity preparedness in the face of escalating attacks, providing a vital safeguard for educational institutions and their stakeholders.

1.3. Aim, Objectives, Significance and Scope of the Study

This study aimed to propose a cybersecurity framework aligned with the ISO/IEC 27001:2022 standard to strengthen cybersecurity in Kenyan universities. It began by investigating cybersecurity threats specific to Kenyan universities, followed by an assessment of existing security controls. The study then crafted a tailored cybersecurity framework to meet the universities' unique needs and aimed to validate its effectiveness.

The research's significance lies in the global forecast of a sharp increase in cybercrime, potentially impacting 85% of organizations worldwide. Most organizations, including universities, lack comprehensive mechanisms to counter these threats. The proposed framework serves as a collaborative model to enhance university cybersecurity, customized for the Kenyan educational context, while bolstering data and information system security. Its adaptability makes it valuable for institutions globally, and it serves as a foundational resource for future cybersecurity framework research.

The study focused on developing effective cybersecurity strategies for chartered Kenyan universities, as identified by the Commission for University Education (CUE). Data collection targeted ICT personnel responsible for critical roles such as system administrators, network security administrators, ERP administrators, and user support.

2. Related Literature

The history of cybersecurity traces its roots back to the 1970s when telephone vulnerabilities were exploited for amusement, leading to the emergence of ARPANET as the precursor to the Internet [12]. In the 1980s, commercial antivirus software was born, while the 1990s saw the proliferation of online threats and the establishment of cybersecurity research institutes. The 2000s marked the internet's widespread accessibility, providing cybercriminals with new opportunities. In the 2010s, high-profile breaches became increasingly common. Today, with greater connectivity and digitization, cybercriminals exploit ransomware and social engineering, resulting in a surge of security breaches, especially in the COVID-19 era [13].

Cybersecurity is undergoing a significant transformation due to several factors, including the growing reliance on information systems and technology in organizations and global economies [14] [15]. This evolution is characterized by the escalating complexity and potential severity of cyberattacks. Recent reports indicate a substantial 125% increase in cybercrime in 2021, driven in part by the rapid adoption of teleworking in response to the COVID-19 pandemic [16]. Despite increased awareness, many organizations struggle to develop effective cybersecurity strategies, necessitating a shift from a defensive stance to a more resilient approach [17]. Challenges in this landscape include resource constraints [18] and the proliferation of specific threats, notably ransomware attacks that have affected various sectors such as education, government, healthcare, and technology [19].

Inadequate adherence to security standards during system configuration and a lack of attention to software updates continue to expose organizations to vulnerabilities [15] [20]. Social engineering exploits human vulnerabilities, often through phishing, presenting an ongoing and formidable threat [18] [21]. The rapid proliferation of Internet of Things (IoT) devices, lacking standardized security measures, introduces new and unique security risks [15] [22]. The increased adoption of cloud storage has led to a surge in vulnerabilities, including misconfigurations, password breaches, and software vulnerabilities [23] [24]. Further complicating matters are the risks associated with mobile devices, lapses in user awareness especially in email phishing, misinterpretations of compliance requirements, external vulnerabilities, and outdated hardware [25].

To address these multifaceted challenges, organizations need to adopt a comprehensive and adaptable cybersecurity approach to safeguard critical infrastructure effectively [26]. This entails shifting from a focus on preventive measures to enablement [26]. Key strategies include the adoption of a zero-trust architecture, continuous authentication and validation of all users, cybersecurity awareness and training, effective patch management, network segmentation, robust access control mechanisms, strong user authentication methods, and secure remote access through virtual private networks (VPNs) [2] [27]-[29]; Additionally, organizations should develop cybersecurity incident response plans,

involve top management in cybersecurity strategy, conduct regular audits, and leverage collaborative applications and mobile devices to enhance their cybersecurity posture [26] [30]. These comprehensive measures collectively contribute to a resilient cybersecurity framework.

Kenya has emerged as a significant player in the digital landscape, attracting global tech giants and cybercriminals alike [16]. However, this technological surge has led to a surge in cybersecurity incidents, with a 133% increase in cyber threats reported since 2021 [7]. In response to these challenges, Kenya has developed a comprehensive cybersecurity governance framework anchored in legislation, the establishment of entities like the National Computer and Cybercrime Coordination Committee (NC4), the National Cybercrime Command Center (NC3), and the Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC), as well as a national cybersecurity strategy (2022-2027). This framework aligns with international best practices and focuses on governance, protection, detection, response, and recovery pillars.

Despite these efforts, Kenya faces a growing cybersecurity threat landscape characterized by ransomware attacks, phishing, distributed denial-of-service attacks, and vulnerabilities in the Internet of Things (IoT). Ransomware gangs, including Conti and Lockbit, target various sectors, particularly those handling critical information [7]. IoT devices have become prime targets, with attackers employing the ransomware for IoT (R4IoT) technique [31]. This escalation can be attributed to increased internet usage, the proliferation of broadband subscriptions, and the adoption of more sophisticated attack tools. A recent cyberattack by Anonymous Sudan on key public offices in Kenya underscores the urgency of bolstering the nation's cybersecurity infrastructure to protect critical data and services [32].

In academia, especially in the post-pandemic era with shifts in content delivery, teleworking, and digital examination methods, cybersecurity has become increasingly challenging [33]. Universities, in particular, are susceptible to cyber threats due to their open and connected nature, continual online presence, legacy technologies, decentralized IT systems, and an information-sharing environment [5] [16] [34]. Cybersecurity incidents in universities are on the rise globally, with ransomware attacks, phishing, and social engineering being prominent threats [17] [35] [36]. These attacks, often underreported to safeguard reputation, have substantial financial and reputational consequences [37]. In Kenya, academic institutions face similar cybersecurity challenges, with sensitive data at risk, particularly financial and examination records [7] [38] [39]. Cybersecurity incidents have led to exam result alterations, financial data tampering, and even illegal hacking activities [10] [22] [40]. These vulnerabilities are exacerbated by universities' lapses in patch management, inadequate security measures, and the proliferation of Bring Your Own Device (BYOD) practices [41].

The NIST Cybersecurity Framework offers a set of guidelines, standards, and best practices for managing cybersecurity risks [42]. It serves as a common lan-

guage and standard for security leaders to assess and enhance organizational cybersecurity resilience [42]. This framework comprises three main components: the "Framework Core," "Framework Implementation Tiers," and "Framework Profile." It offers a comprehensive approach to cybersecurity, divided into five functions: Identify, Protect, Detect, Respond, and Recover (National Institute of Standards and Technology, 2022). ISO/IEC 27001:2022 serves as a reference guide for establishing and implementing information security controls based on ISO/IEC 27001:2022. It offers generic cybersecurity controls and guidance on their implementation, aiding organizations in creating customized cybersecurity frameworks [43]. The standard categorizes its 93 controls into four thematic areas: People, Physical, Technological, and Organizational Controls (ISO/IEC, 2022). These frameworks provide invaluable guidance for managing cybersecurity risks, with NIST's framework offering a holistic approach based on functions and categories, and ISO/IEC 27001:2022 providing specific controls and thematic areas. Together, they help organizations establish robust cybersecurity practices and resilience in an ever-evolving digital landscape.

3. Research Methodology

This study adopted a systematic methodology to enhance cybersecurity in Kenyan universities, detailing the procedures for research design, data collection, and analysis. Utilizing a descriptive research design, the study aimed to gather quantitative data relevant to cybersecurity practices, ERP implementation, and cyber threats in Kenyan universities. The Design Science Research Methodology (DSRM) was employed to develop and validate a cybersecurity framework tailored to Kenyan universities, following the steps outlined by [44].

The target population included 35 public and 25 private universities accredited by the Commission for University Education. A sample size of 48 respondents, consisting of system administrators and cybersecurity experts, was determined using [45] formula, with purposive sampling ensuring specialized insights into cybersecurity practices.

Data was collected via an online questionnaire, which was pilot-tested for reliability and validity, ensuring dependable and accurate results. The questionnaire covered professional details of respondents, cybersecurity best practices, ERP implementation, cyber threats, and existing controls. Reliability was measured using internal consistency, yielding a Cronbach's Alpha of 0.705, indicating high reliability. Content and face validity were confirmed through expert evaluations.

Quantitative data was analyzed using SPSS, producing descriptive statistics such as frequencies, percentages, mean, and standard deviation. Results were presented in pie charts, bar graphs, and tables. Mean values were interpreted to categorize the severity of cybersecurity threats.

Ethical considerations were meticulously addressed, ensuring informed consent and confidentiality for all respondents. The study's methodology provided a

comprehensive framework for understanding and enhancing cybersecurity in Kenyan universities, with recommendations for comparative studies to identify and adapt best practices from other contexts.

4. Results and Discussion

The study examined cybersecurity challenges in Kenyan universities, with data collected from 45 institutions, achieving a 93.75% response rate from ICT professionals. Most respondents (57%) had 6 - 10 years of experience, and 74% were not affiliated with cybersecurity professional bodies. Findings revealed that 66% of universities implemented international standards, with ISO/IEC 27001 being prominent. All had operational Enterprise Resource Planning (ERP) systems, and 40% used cloud services. Additionally, 74% offered open and distance learning (ODeL), and 68% implemented teleworking. The study quantified cybersecurity threats using a Likert scale. Notable concerns, as per Table 1 included outdated technology (mean 3.69) and unpatched software (mean 3.51) posing the highest risks. Lower threats include cloud vulnerabilities (mean 2.22) and machine learning attacks (mean 2.2), indicating varying levels of preparedness and risk across different areas.

Table 1. Cybersecurity threats at Kenyan universities.

Cybersecurity threats	No extent		Small extent		Moderate extent		Large extent		Very large extent		Mean
	Freq.	(%)	Freq.	(%)	Freq.	(%)	Freq.	(%)	Freq.	(%)	
Outdated/obsolete technology	5	11.11	6	13.33	6	13.33	9	20.00	19	42.22	3.69
Unpatched and outdated software	6	13.33	4	8.89	8	17.78	15	33.33	12	26.67	3.51
Obsolete antiviruses	8	17.78	6	13.33	8	17.78	8	17.78	15	33.33	3.36
BYOD/Mobile device vulnerabilities	6	13.33	9	20.00	4	8.89	17	37.78	9	20.00	3.31
Social engineering/phishing	2	4.44	14	31.11	10	22.22	9	20.00	10	22.22	3.24
Insider threat by employees	10	22.22	6	13.33	4	8.89	14	31.11	11	24.44	3.22
Theft of computing devices	10	22.22	9	20.00	5	11.11	12	26.67	9	20.00	3.02
Ransomware	12	26.67	8	17.78	5	11.11	12	26.67	8	17.78	2.91
Misuse of the Internet of Things	19	42.22	5	11.11	3	6.67	9	20.00	9	20.00	2.64
Data breaches and poor data management	12	26.67	13	28.89	9	20.00	6	13.33	5	11.11	2.53
Cloud vulnerabilities	22	48.89	7	15.56	5	11.11	6	13.33	5	11.11	2.22
Machine learning and AI attacks	18	40.00	13	28.89	6	13.33	3	6.67	5	11.11	2.2
Software/Misconfiguration vulnerabilities	17	37.78	12	26.67	10	22.22	3	6.67	3	6.67	2.18
Third-party vulnerabilities	20	44.44	12	26.67	6	13.33	4	8.89	3	6.67	2.07
Distributed denial of service	14	31.11	18	40.00	12	26.67	0	0.00	1	2.22	2.02
SQL Injections	19	42.22	15	33.33	8	17.78	0	0.00	3	6.67	1.96

Cybersecurity controls were categorized into organizational, human, physical, and technological. As per Table 2, 62.22% of respondents agreed or strongly agreed that ICT staff engage with security forums (mean 3.47). Conversely, only 20% agreed or strongly agreed that adequate resources are allocated to cybersecurity activities (mean 2.07), and 26.67% agreed or strongly agreed on maintaining contact with cybersecurity authorities (mean 2.27), highlighting significant gaps.

Table 2. University's organizational controls.

University's organizational controls	Strongly disagree		Disagree		Neutral		Agree		Strongly agree		Mean
	Freq	(%)	Freq	(%)	Freq.	(%)	Freq.	(%)	Freq	(%)	
ICT staff contact with special interest groups	8	17.78	6	13.33	3	6.67	13	28.89	15	33.33	3.47
Protection of critical information assets:	8	17.78	10	22.22	3	6.67	14	31.11	10	22.22	3.18
Cloud computing risks	11	24.44	9	20.00	3	6.67	10	22.22	12	26.67	3.07
Access rights policy/procedure	9	20.00	16	35.56	3	6.67	9	20.00	8	17.78	2.80
Management of authentication information	12	26.67	13	28.89	3	6.67	8	17.78	9	20.00	2.76
Cybersecurity in ERP acquisition	13	28.89	14	31.11	1	2.22	8	17.78	9	20.00	2.69
Business continuity plan	14	31.11	12	26.67	1	2.22	12	26.67	6	13.33	2.64
Legal, regulatory compliance	10	22.22	15	33.33	1	2.22	15	33.33	4	8.89	2.73
Review and audit of infrastructure	13	28.89	15	33.33	3	6.67	9	20.00	5	11.11	2.51
Third-party risk management	13	28.89	17	37.78	1	2.22	9	20.00	5	11.11	2.47
Privacy and PII protection	15	33.33	13	28.89	3	6.67	8	17.78	6	13.33	2.49
Cybersecurity policies	13	28.89	18	40.00	1	2.22	8	17.78	5	11.11	2.42
Cybersecurity risk assessment	14	31.11	18	40.00	3	6.67	6	13.33	4	8.89	2.29
Contact with cybersecurity authorities	18	40.00	12	26.67	3	6.67	9	20.00	3	6.67	2.27
Threat intelligence analysis	21	46.67	10	22.22	1	2.22	10	22.22	3	6.67	2.20
Resource allocation for cybersecurity	21	46.67	12	26.67	3	6.67	6	13.33	3	6.67	2.07

In human controls in Table 3, only 34.29% of respondents agreed or strongly agreed that regular cybersecurity awareness and training are conducted (mean 2.51). Awareness of cybersecurity responsibilities was agreed or strongly agreed by just 25.71% (mean 2.20), and clear reporting mechanisms were agreed or strongly agreed by 25.71% (mean 2.26).

Physical controls as per Table 4 received mixed satisfaction in Kenyan universities. Only 40% agreed or strongly agreed that adequate physical security

Table 3. Human cybersecurity controls.

Human cybersecurity controls	Strongly disagree		Disagree		Neutral		Agree		Strongly agree		Mean
	Freq.	(%)	Freq.	(%)	Freq.	(%)	Freq.	(%)	Freq.	(%)	
Cybersecurity awareness and training: Regular training and updates for staff and stakeholders.	15	34.29	13	28.57	1	2.86	9	20.00	6	14.29	2.51
Cybersecurity responsibilities awareness: Staff know their cybersecurity duties and policy violation consequences.	19	42.86	13	28.57	1	2.86	8	17.14	4	8.57	2.20
Reporting mechanism: Clear channels for reporting cybersecurity incidents promptly.	17	37.14	14	31.43	3	5.71	9	20.00	3	5.71	2.26

Table 4. Physical cybersecurity controls.

Physical cybersecurity controls	Strongly disagree		Disagree		Neutral		Agree		Strongly agree		Mean
	Freq.	(%)	Freq.	(%)	Freq.	(%)	Freq.	(%)	Freq.	(%)	
There are adequate physical security controls in areas containing critical and sensitive information	12	25.71	13	28.57	3	5.71	10	22.86	8	17.14	2.82
Procedure for people accessing secure areas such as server room have been established and implemented	8	17.14	14	31.43	4	8.57	6	14.29	13	28.57	3.04

exists in areas with sensitive information (mean 2.82). Meanwhile, 42.86% agreed or strongly agreed that access procedures to secure areas like server rooms are established and implemented (mean 3.04).

Technological controls in Table 5 addressed mobile device security (40% identified risks), privileged access rights (31.43% controlled), malware protection (25.71% implemented), security configurations (31.43% secured networks), data masking (11.43% implemented), back-up copies (20% maintained), event logging (31.43% implemented), monitoring activities (34.28%), software installations control (20%), network security (57.14%), and web filtering (28.58%). Technical vulnerabilities were managed by 40%.

Table 5. Technological cybersecurity controls.

Technological cybersecurity controls	Strongly disagree		Disagree		Neutral		Agree		Strongly agree		Mean
	Freq.	(%)	Freq.	(%)	Freq.	(%)	Freq.	(%)	Freq.	(%)	
Network security: Secured and controlled to protect information	6	14.29	12	25.71	1	2.86	14	31.43	12	25.71	3.29
ERP vulnerabilities: Identified and mitigated with controls	9	20.00	15	34.29	3	5.71	9	20.00	9	20.00	2.86

Continued

Mobile device risks: Managed and controlled	13	28.57	12	25.71	3	5.71	10	22.86	8	17.14	2.74
Monitoring systems: Anomalous behavior monitored; incidents evaluated	14	31.43	12	25.71	4	8.57	8	17.14	8	17.14	2.63
Privileged access: Restricted, monitored, and managed	10	22.86	17	37.14	4	8.57	9	20.00	5	11.43	2.60
Security configurations: Established, documented, and reviewed	14	31.43	13	28.57	4	8.57	8	17.14	6	14.29	2.54
Log management: Logs produced, protected, and analyzed	15	34.29	13	28.57	3	5.71	6	14.29	8	17.14	2.51
Website access: Managed to reduce malicious content exposure	18	40.00	10	22.86	4	8.57	6	14.29	6	14.29	2.40
Malware protection: Implemented with user awareness	17	37.14	14	31.43	3	5.71	8	17.14	4	8.57	2.29
Backups: Regularly tested and maintained	13	28.57	19	42.86	4	8.57	5	11.43	4	8.57	2.29
Software installation: Controlled on operational systems	17	37.14	18	40.00	1	2.86	6	14.29	3	5.71	2.11
Data masking: Limits exposure of sensitive data and ensures compliance	18	40.00	21	45.71	1	2.86	4	8.57	1	2.86	1.89

The findings highlight cybersecurity challenges in Kenyan universities, revealing significant threats from outdated technology and unpatched software. While many universities implement international standards, gaps remain in resource allocation, cybersecurity awareness, and physical security. Technological controls show varied effectiveness, indicating a need for comprehensive improvements across all areas.

5. Proposed Cybersecurity Framework for Kenyan Universities in Conformity with ISO/IEC 27001:2022 Standard

The proposed cybersecurity framework for Kenyan universities as per Figure 1, is a comprehensive strategy aimed at enhancing information security and protecting critical assets and processes. This framework comprises several crucial phases, beginning with understanding the university's context, core mission, goals, and stakeholder expectations. This contextual awareness ensures alignment with the university's mission and helps identify specific risks and priorities. The subsequent phase involves identifying critical assets and processes, allowing for a focused and strategic approach to protecting the most valuable components of the university's operations. Threat assessments, attack vectors, and vulnerability analyses follow to understand potential risks comprehensively. Cybersecurity risk analysis and evaluation come next, assessing the likelihood

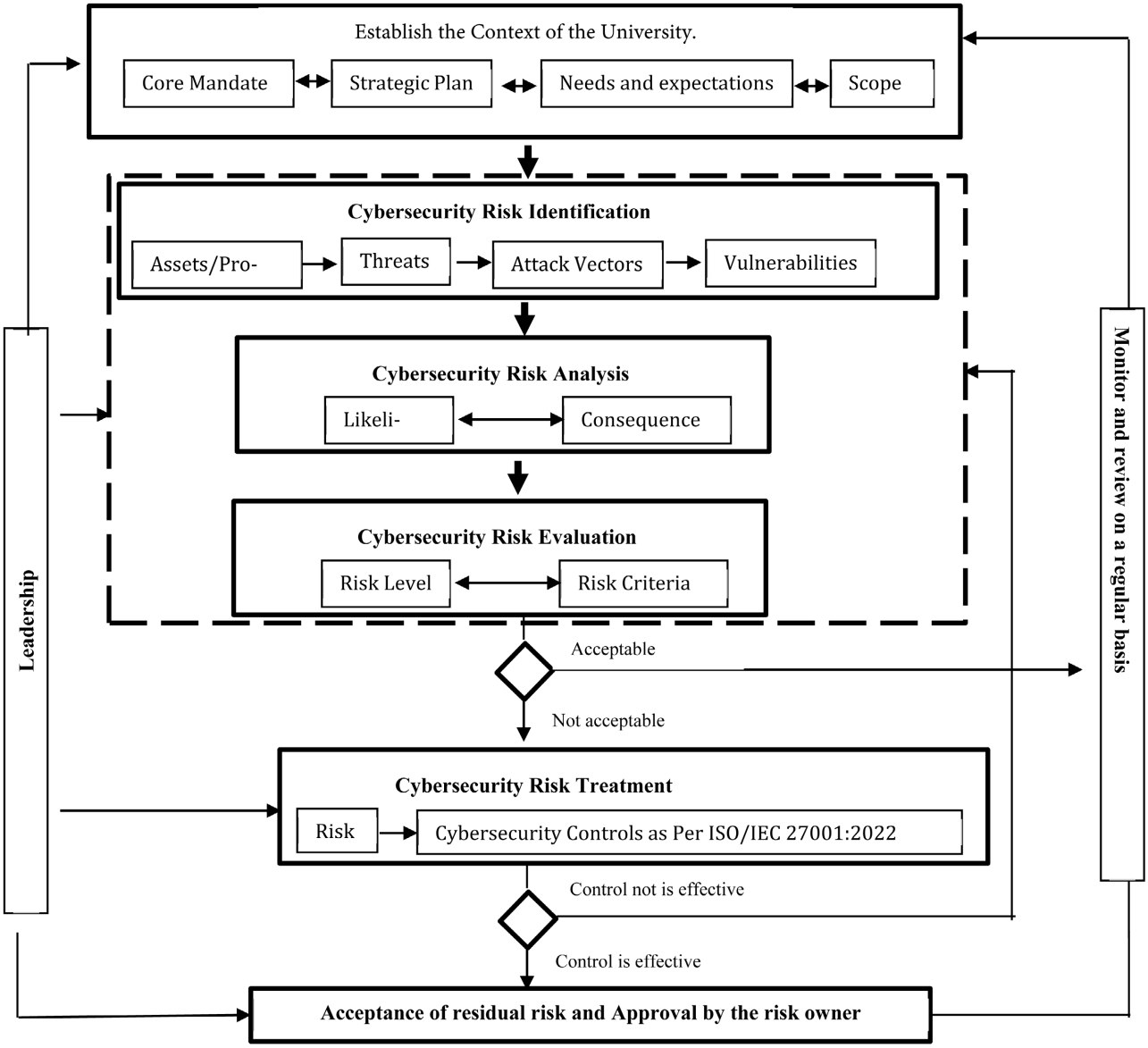


Figure 1. Proposed cybersecurity framework for Kenyan universities in conformity with ISO/IEC 27001:2022 standard.

and consequences of identified risks, facilitating prioritization, resource allocation, and risk mitigation strategies. Risk treatment is the subsequent step, where chosen measures are implemented to mitigate identified risks, both technical and non-technical controls. Acceptance and approval of residual risks ensure that any remaining risks are acknowledged and managed within acceptable limits. Ongoing monitoring and review processes adapt to evolving threats and assess the effectiveness of security measures. Leadership plays a vital role in fostering a culture of cybersecurity awareness, providing direction, allocating resources, and supporting compliance and incident response efforts. The proposed cybersecurity framework equips Kenyan universities to proactively manage cybersecurity risks, align with institutional goals, protect critical assets, and maintain a resilient information security posture. The framework emphasizes con-

tinuous improvement and adapts to the evolving threat landscape, ultimately strengthening the overall cybersecurity posture of these educational institutions.

The proposed cybersecurity framework for Kenyan universities is designed to address current cybersecurity threats in the unique university environment. It draws from internationally recognized best practices, such as ISO/IEC 27001 and the NIST cybersecurity framework. Tailored for Kenyan universities, the framework covers all aspects of cybersecurity, from identifying information assets to risk assessment, treatment, monitoring, and compliance with legal requirements. This framework is well-aligned with the universities' adoption of technologies like ERP, cloud computing, and mobile technologies. It also allows for continual improvement by accommodating periodic reviews and updates to adapt to emerging threats and organizational changes. In summary, the proposed framework offers a robust approach to enhancing cybersecurity management in Kenyan universities, addressing their specific needs and challenges.

6. Key Findings

The study focused on cybersecurity practices among Kenyan universities, revealing significant trends and challenges. It found that 66% of these institutions have adopted international standards like ISO/IEC 27001:2013 and CIS Controls for cybersecurity risk management. Technological advancements were evident with ERP systems, cloud services, ODeL programs, and teleworking becoming commonplace. Despite 71% having cybersecurity policies, only 29% fully implemented them. Over five years, 74% experienced cyberattacks, mostly mild to moderate, resolved within 24 hours, yet reporting to authorities occurred in only 69% of cases.

Cybersecurity threats were categorized into critical (e.g., outdated technology, insider threats), moderately critical (e.g., ransomware, data breaches), and slightly critical (e.g., SQL injections). These threats stemmed from organizational, technological, physical, and human factors, exacerbated by resource constraints and inadequate ICT investment. Organizational controls were notably deficient, impacting cybersecurity preparedness. Human controls highlighted gaps in awareness and training, while physical controls were lacking in critical information areas.

Technological controls showed varied implementation levels, underscoring needs in mobile device security, malware protection, and network management. A proposed cybersecurity framework aligned with ISO/IEC 27001:2022 aimed to mitigate these challenges. It encompassed phases from risk identification to continuous monitoring, addressing critical cybersecurity areas and international best practices. Evaluation confirmed its alignment with standards, ability to manage risks, and integrate with organizational processes, stressing compliance and continual improvement.

Overall, the study emphasizes enhancing policy implementation, bolstering cybersecurity controls, and adopting frameworks to fortify resilience against

evolving threats in Kenyan universities. These insights underscore the imperative for comprehensive cybersecurity strategies to safeguard academic institutions effectively.

7. Conclusion

This study aimed to bolster cybersecurity in Kenyan universities by developing an ISO/IEC 27001:2022-aligned framework. Findings indicate room for improvement in implementing international standards, as cyberattacks remain prevalent, often due to limited resources and inadequate technology investment. Full policy implementation and strengthening of organizational, human, physical, and technological controls are crucial to mitigate these threats effectively. This research contributes valuable insights for policymakers, administrators, and cybersecurity professionals seeking to enhance security practices in the academic sector. One significant challenge faced during the study was ensuring respondent anonymity while collecting genuine feedback. In conclusion, the escalating cyber threats emphasize the necessity of implementing a robust, university-specific cybersecurity framework tailored to Kenyan universities' specific needs to safeguard digital assets effectively.

8. Recommendations

Based on the study's findings, Kenyan universities should prioritize full implementation of cybersecurity policies, increase investment in information technologies to address resource shortages and outdated systems, and enhance organizational controls through regular risk assessments and cybersecurity awareness programs. Attention should also be given to improving physical security measures and adopting a comprehensive cybersecurity framework aligned with ISO/IEC 27001 standard. Further research should evaluate the impact of international standards on cybersecurity, explore resource constraints, and assess the effectiveness of policy implementation, awareness programs, and reporting mechanisms. Comparative studies with foreign universities can offer insights into best practices for adapting and improving cybersecurity measures in Kenyan institutions.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Powell, O. (2022) The Biggest Data Breaches and Leaks of 2022.

[2] Check Point (2022) Check Point Software 2022 Security Report.

[3] Miller, E. (2022) The State of Cybersecurity in Higher Education: Top Insights and Trends.

[4] Colaco, S. (2022) Cybersecurity in Education. https://kitaboo.com/how-educational-institutions-mitigate-cybersecurity-threats-in-education/

[5] Campbell, S. (2017) Cybersecurity in Higher Education: Problems and Solutions. https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education

[6] Choo, K.-K.R., Takakura, H., Lee, R. and Lee, K.T. (2023) Cybersecurity in the Higher Education Sector: Challenges, Solutions and Best Practices. *Organizational Cybersecurity Journal*, **26**, 2-9.

[7] CAK (2022) Cybersecurity Quatery Report.

[8] Wanjau, M. (2020) The State of Cybercrime in the ICT Sector.

[9] Palmer, D. (2022) Ransomware Attacks Are Hitting Universities Hard, and They Are Feeling the Pressure. https://www.zdnet.com/article/ransomware-attacks-are-hitting-universities-hard-and-they-are-feeling-the-pressure/

[10] Teng'o, S. (2017) Cyber Security: Rise of the Student Hacker. https://www.standardmedia.co.ke/ureport/article/2001239325/cyber-security-rise-of-the-student-hacker

[11] Aineah, A. (2018) Clueless Varsities Rewarding Hackers with Top Grades. https://www.standardmedia.co.ke/article/2001268939/why-research-puts-kenyan-students-fourth-on-list-of-top

[12] Matara, E. (2023) Kabarak University Recovers Hacked Facebook Account.

[13] Nayak, U. and Rao, U.H. (2014) The InfoSec Handbook: An Introduction to Information Security. Apress.

[14] Minnaar, A. and Herbig, F.J. (2022) Cyberattacks and the Cybercrime Threat of Ransomware to Hospitals and Healthcare Services during the COVID-19.

[15] European Economic and Social Committee (2018) Cybersecurity: Ensuring Awareness and Resilience of the Private Sector Across Europe in Face of Mounting Cyber Risks Study. https://www.eesc.europa.eu/en/our-work/publications-other-work/publications/cybersecurity-ensuring-awareness-and-resilience-private-sector-across-europe-face-mounting-cyber-risks-study#:~:text=Share4-,Cybersecurity%3A%20Ensuring%20awareness%20and%20resili

[16] Jaccard, J.J. and Nepal, S. (2014) A Survey of Emerging Threats in Cybersecurity. *Journal of Computer and System Sciences*, **80**, 973-993.

[17] World Economic Forum (2022) Global Cybersecurity Outlook 2022.

[18] Chapman, J. (2022) Latest Cyber Impact Report Underlines Ransomware as a Huge Threat, but Financial Cost of Attacks Is Still Unclear. https://www.jisc.ac.uk/blog/latest-cyber-impact-report-underlines-ransomware-as-a-huge-threat-20-apr-2022#

[19] Koziol, J., Watts, R. and Bottorff, C. (2023) Most Common Cyber Security Threats. https://www.forbes.com/advisor/business/common-cyber-security-threats/

[20] Blackfog (2022) The New Standard in Cybersecurity.

[21] Andress, J. (2014) The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. 2nd Edition, Syngress.

[22] Wang, Z.G., Zhu, H.S., Liu, P.P. and Sun, L.M. (2021) Social Engineering in Cybersecurity: A Domain Ontology and Knowledge Graph Application Examples. *Cybersecurity*, **4**, Article No. 31.

[23] Aubly, C., Bowen, E. and Frank, W. (2021) Cyber AI: Real Defense. https://www.deloitte.com/global/en/our-thinking/insights/topics/technology-management/tech-trends/2022/future-of-cybersecurity-and-ai.html

[24] Kaspersky (2021) What is Cloud Security? https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security

[25] IBM (2021) 2021 IBM Security X-Force Cloud Threat Landscape Report.

[26] USA Government (2022) Stop Ransomware. https://www.cisa.gov/stopransomware

[27] KPMG (2022) Cyber Security Considerations 2022: Trust through Security.

[28] Akali, H. (2002) Zero Trust Architecture: Adoption, Benefits, and Best Practices. https://www.cyberdefensemagazine.com/zero-trust-architecture-2/

[29] National Institute of Standards and Technology (2020) Zero Trust Architecture NIST Special Publication 800-207.

[30] Kay, A., Hutcherson, C., Keene, C., Zhang, X. and Terwillig, M. (2021) How Financial Institutions Address Cybersecurity Threats: A Critical Analysis. *Issues in Information Systems*, **22**, 63-74.

[31] Vijayalakshm, B. and Sailaja, M. (2016) A Study on Contemporary Challenges and Opportunities of Retail Banking in India. *Global Journal of Finance and Management*, **8**, 131-141.

[32] Modgil, S., Dwivedi, Y.K., Rana, N.P., Gupta, S. and Kamble, S. (2022) Has Covid-19 Accelerated Opportunities for Digital Entrepreneurship? An Indian Perspective. *Technological Forecasting and Social Change*, **175**, Article 121415. https://doi.org/10.1016/j.techfore.2021.121415

[33] Cloudflare (2023) What is Anonymous Sudan?

[34] Lang, M.A. and Connolly, L.Y. (2021) Managing the Cybersecurity Risks of Teleworking in the Post-Pandemic "New Normal".

[35] Engel, B. (2020) The History of the Internet and the Colleges That Built It. https://edtechmagazine.com/higher/article/2013/11/history-internet-and-colleges-built-it

[36] Alawida, M., Omolara, A.E., Abiodun, O.I. and Al-Rajab, M. (2022) A Deeper Look into Cybersecurity Issues in the Wake of Covid-19: A Survey. *Journal of King Saud University*: *Computer and Information Sciences*, **34**, 8176-8206. https://doi.org/10.1016/j.jksuci.2022.08.003

[37] Jideani, P., Leenen, L., Alexander, B. and Barnes, J. (2018) Towards an Electronic Retail Cybersecurity Framework. 2018 *International Conference on Advances in Big Data*, *Computing and Data Communication Systems*, Durban, 06-07 August 2018, 1-6. https://doi.org/10.1109/icabcd.2018.8465428

[38] Onapsis (2022) ERP Security: The Reality of Business Critical Application Protection.

[39] Nasongo, N. (2021) Expert Decries Increase in Cyber Attacks during Covid-19.

[40] Law, K. (2019) Denis Wahome Muriithi v Kenyatta University [2021] eKLR. http://kenyalaw.org/caselaw/cases/view/215634

[41] Kitheka, P. (2013) Information Security Management System in Public Universities in Kenya: A Gap Analysis between Common Practices and Industrial Best Practices.

[42] Dillon, R., Lothian, P., Grewal, S. and Pereira, D. (2021) Cyber Security: Evolving Threats in an Ever-Changing World. In: Adrian, T.H. and Kuah, R.D., Eds., *Digital Transformation in a Post-Covid World*: *Sustainable Innovation*, *Disruption and Change*, CRC Press, 129-154. https://doi.org/10.1201/9781003148715-7

[43] ISO/IEC (2022) Information Security, Cybersecurity and Privacy Protection—Information Security Controls.

[44] Fontes, E.L.G. and Balloni, A.J. (2007) Security in Information Systems: Sociotechnical Aspects. *Innovation and Advanced Techniques in Computer and Information Science and Engineering*, **2007**, 163-166.

[45] Denyer, D. and Tranfied, D. (2009) Producing a Systematic Review. In: Buchanan, D.A. and Bryman, A., Eds., *The Sage Handbook of Organizational Research Methods*, Sage Publications, 671-689.