JISTaP https://www.jistap.org
Journal of Information Science Theory and Practice

RESEARCH PAPER
J Inf Sci Theory Pract 14(2): 1-25, 2026

eISSN : 2287-4577 pISSN : 2287-9099

https://doi.org/10.1633/JISTaP.2026.14.2.1

Bridging the Gaps in Information Security Risk Management in Higher Education: Challenges, Best Practices, and Future Directions

Ruon Kueth Bum
Faculty of Computing & Software Engineering, Arba Minch University, Arba Minch, Ethiopia
E-mail: ruombuom12@gmail.com

Kibreab Adane*
Faculty of Computing & Software Engineering, Arba Minch University, Arba Minch, Ethiopia
E-mail: kibreinfo@gmail.com

Mohammed Abebe
Faculty of Computing & Software Engineering, Arba Minch University, Arba Minch, Ethiopia
E-mail: moshethio@gmail.com

Mesay Samuel
Faculty of Computing & Software Engineering, Arba Minch University, Arba Minch, Ethiopia
E-mail: mess.sama@gmail.com

Durga Prasad Sharma
Faculty of Computing & Software Engineering, Arba Minch University, Arba Minch, Ethiopia
E-mail: dp.shiv08@gmail.com

ABSTRACT

Higher education institutions (HEIs) are becoming a breeding ground for hackers due to their open culture policies and the volume of sensitive data they produce. Unless an appropriate information security risk management (ISRM) framework is in place to support them in thriving in the digital era, African HEIs in general and Ethiopian HEIs in particular are not immune to the expanding cybersecurity threats. This study aims to identify existing gaps, best practices, and future directions regarding ISRM in HEIs in Ethiopia. To achieve its core objective, the study adopted an exploratory research design and leveraged quantitative and qualitative approaches. Online and offline survey questions were distributed by email and in person, respectively, to collect quantitative data. Academic and information and communication technology (ICT) staff personnel from four different HEIs were chosen using the purposive sample technique. The qualitative data were gathered from relevant research and an interview with the ICT directors. The topics covered by the data collection tool were adopted from recent international information security frameworks and standards. Microsoft Excel 2016 (Microsoft, Redmond, WA, USA) was used for data analysis. Even though there are some acceptable secure practices in the studied HEIs, secure online and offline practices are still lacking in the areas of organizational, people, physical, and technology controls. To address the aforementioned concerns, the study proposes an appropriate ISRM Framework for HEIs to mitigate unauthorized access, use, disclosure, alteration, or deletion of valuable information, although the framework was not put into practice or transformed into a prototype or simulation-based demonstration.

Keywords: information security risk management framework, information security policy in higher education, information security in Ethiopian higher education, risk identification, risk assessment, risk mitigation

Received: April 18, 2025 **Revised:** February 5, 2026
Accepted: February 27, 2026 **Published:** June 30, 2026

***Corresponding Author:** Kibreab Adane
https://orcid.org/0000-0002-3021-5059
E-mail: kibreinfo@gmail.com

All JISTaP content is Open Access, meaning it is accessible online to everyone, without fee or authors' permission. Open Access articles are automatically archived in the Korea Institute of Science and Technology Information (KISTI)'s Open Access repository (AccessON). All JISTaP content is published and distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/). Under this license, the authors retain full ownership of their work, while permitting anyone to use, distribute, and reproduce the content in any medium, as long as the original authors and source are cited. For any reuse, redistribution, or reproduction of a work, users must clarify the license terms under which the work was produced.

© 2026 [Ruon Kueth Bum, Kibreab Adane, Mohammed Abebe, Mesay Samuel, Durga Prasad Sharma] This article is distributed under the Creative Commons Attribution License (CC BY), allowing unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited. It is published by the Korea Institute of Science and Technology Information & Yonsei University's Research Institute for Academic Library Development.

1. INTRODUCTION

Information security is the process of protecting and preserving private or sensitive data so that it is not compromised by unauthorized access, use, disclosure, disruption, alteration, or erasure. Safeguarding sensitive information requires the adoption of numerous strategies to preserve confidentiality, integrity, and availability (Alhassan & Adjei-Quaye, 2017).

Higher education institutions (HEIs) are the least secure places in the universe when compared to other organizations because of allowing Bring Your Own Devices (BYOD), as they produce legal documents like degree certificates, experience growing student enrolments, hold a large number of hardcopy and softcopy sensitive materials with inadequate IT security and data protection mechanisms, and are a fertile ground for IT exploration and publicly open innovation platforms (Adane, 2020; Bongiovanni, 2019).

Information security breaches occur in both developed and developing countries' HEIs. For example, Several HEIs in the USA, notably Georgia Institute of Technology (March 2019), the University of Washington (February 2019), the University of Utah (June 2018), and the University of Vermont (May 2018), have recently reported information security breaches. Internal database attacks compromised about 1.3 million Georgia Institute of Technology records; human error compromised about 1 million University of Washington personal health records; electronic equipment theft at the University of Utah resulted in the loss of 607 patients' personal information; and a security breach at the University of Vermont that affected NetID, the university's online services portal, may have compromised the personal information of 37,000 current and former faculty, staff, and students (Bongiovanni, 2019). Alenezi (2024) revealed that HEIs in South Africa (Tshwane University of Technology, January 2024), Argentina (University of Buenos Aires, December 2023), the Philippines (De La Salle University, October 2023), and Brazil (Universidade Federal de Mato Grosso do Sul, September 2023) have been the target of cyberattacks in recent years.

HEIs are supposed to protect sensitive data and ensure its confidentiality, integrity, and accessibility (Kombo et al., 2023). According to Keefa et al. (2024), insider threats, inadequately implemented information security frameworks, BYOD policy, and a lower investment in information security were among the main vulnerabilities in HEIs. In another study, Keefa et al. (2024) stated that poor security management, significant employee turnover, a general lack of enthusiasm for information security, human factors, work settings, and technology are some of the major challenges affecting information security in HEIs.

Alenezi (2024) conducted a systematic review considering research publications from 2014 to 2024 on cybersecurity risks and strategies in HEIs in developing and emerging countries, which included authors from Morocco, China, the Philippines, Moldova, India, Ecuador, Ghana, Indonesia, Turkey, Malaysia, and Jordan. The author review finding reveals the following key gaps: i) a lack of cybersecurity research focusing on the particular challenges of African universities, ii) a lack of longitudinal studies to evaluate the long-term effects of International Organization for Standardization (ISO) 27001 implementation, iii) a lack of comparative studies on information security considering diverse educational institutions, iv) a lack of cybersecurity education programs, and iv) insufficient evaluations of how cybersecurity training affects actual security outcomes. Nkambule and Jansen van Vuuren (2024) stated that African HEIs lack a thorough legislative framework for cybersecurity, experience insufficient financial resources and cybersecurity competence, and lack cybersecurity awareness or hygiene among users. The authors suggest that institutions must keep pace with evolving threats, prioritize cybersecurity, and implement effective plans.

Addressing the aforementioned challenges requires developing a comprehensive information risk management framework. The field of information security risk management (ISRM) encompasses the methodical process of detecting, evaluating, and mitigating potential risks to the organization's important data assets (Daimi & Peoples, 2021). These processes include the following elements.

Risk identification: This phase includes locating potential threats and vulnerabilities against an organization's information assets. It encompasses analyzing both internal and external factors, conducting risk assessments, and taking into account various components like technology, processes, and human factors.

Risk assessment: In prioritizing their efforts to mitigate recognized risks, organizations assess the likelihood and consequences of such risks. In this step, the possible effects of a risk occurrence are evaluated, and the organization's tolerance for such risks is established.

Risk mitigation: Companies put controls and procedures in place to lessen the possibility and effect of hazards that have been recognized. This includes implementing

 https://doi.org/10.1633/JISTaP.2026.14.2.1

technical controls, establishing procedures and guidelines, conducting recurring security awareness training, and ensuring compliance with relevant laws and standards.

Risk monitoring and review: Companies keep an eye on and evaluate the performance of their information security procedures on a constant basis. This includes conducting regular vulnerability assessments, conducting penetration tests, keeping an eye on security logs, and developing incident response strategies.

Compliance and legal considerations: It is morally required of organizations to consider the legal and regulatory aspects of information security compliance. This requires a careful understanding of both industry-specific legislation and data protection laws.

Poor information management, noncompliance with acceptable standards and laws for risk management, and the inability to identify sources of threats and vulnerabilities were some of the challenges in HEIs (Kombo et al., 2023). Like many other HEIs worldwide, HEIs in Ethiopia are vulnerable to a variety of information security threats that jeopardize the availability, confidentiality, and integrity of digital assets. In this regard, Ejerssa (2018) revealed insufficient information security controls, a lack of clear and uniform information technology governance, and immaturity in the application of information security measures in the HEIs of Ethiopia, despite not developing an ISRM framework. Abebe (2022) revealed a lack of knowledge and comprehension among academic personnel, employees, and scholars about the protection of information, its assurance, and the safeguarding of computer systems in the selected public organizations in Ethiopia, despite not developing an ISRM framework.

Although they do not consider ISRM in Ethiopian HEIs, related studies (Ansari & Ali, 2021; Araújo et al., 2025; Baleid & Abdullah, 2026; Bongiovanni, 2019; Dawar & Shivarama, 2017; Ganesen et al., 2022; Joshi & Singh, 2017; Kiura & Mango, 2017; Njoroge et al., 2019; Putri & Wijaya, 2023; Sikman et al., 2023; Suroso & Fakhrozi, 2018) conducted assessments on ISRM in HEIs. Our study sought to fill in gaps in the literature by utilizing a variety of the latest and most popular ISRM frameworks, standards, and best practices from the viewpoint of people, physical, organizational, and technological controls. To improve generalizability, other researchers looking into ISRM may choose to employ the data collection tools and research findings from our study.

In short, the core contributions of the study are fourfold.

- Review popular International Information Security Management Frameworks, Standards, and Best Practices to assess ISRM Practices in HEIs of Ethiopia.
- Identify current gaps and best practices in managing information security risks from the viewpoint of people, physical, organizational, and technological controls.
- Develop a comprehensive ISRM framework for HEIs in Ethiopia.
- Compare the proposed framework with the related studies' frameworks to illustrate the unique contributions of the study.

2. RELATED WORKS

While various countries have adopted diverse strategies to safeguard their respective university environments, a notable gap in research studies addressing this domain within the localized context of HEIs in Ethiopia is evident. This paucity of scholarly endeavors investigating ISRM practices in Ethiopian higher education presents a significant gap in the existing body of knowledge.

Ejerssa (2018) assessed the maturity level of information security within some of the public universities in Ethiopia and revealed the presence of information security risks that need to be addressed. Sikman et al. (2023) proposed a model for establishing and operating a durable system for managing information security in HEIs, despite not delving into the particular challenges and risks encountered by said institutions. Putri and Wijaya (2023) focus on minimizing the occurrence and impact of various information technology risks in Indonesian educational institutions, despite not assessing the risk of lacking information policies and training employees.

Ganesen et al. (2022) focus on the necessity for the higher education sector to adopt a cybersecurity risk appraisal methodology to protect its information technology infrastructure from cyberattacks, despite the failure of the sector to explicitly advocate for continuous monitoring, assessment, and enhancements to counteract emerging risks. Bongiovanni (2019) identifies seven primary subjects discussed in the literature, such as risk management frameworks, standards, technical solutions for cyber-related issues, governance systems for information security management, and the need for additional research on information security culture within HEIs.

Sulistyowati and Hari Ginardi (2018) highlight the importance of addressing vulnerabilities in websites and In-

ternet networks in academic environments. However, the applicability of the methodology needs to be investigated in different academic settings for adaptability. Njoroge et al. (2019) designed a framework that aims to address the gaps in current security practices and align universities' security risks, but the study needs to be expanded by investigating the impacts of information security breaches on the academic and administrative functions of universities. Suroso and Fakhrozi (2018) used a framework for assessing and addressing threats to information systems, despite not providing detailed guidance on selecting and applying safeguards and mitigation strategies for identified risks.

Joshi and Singh (2017) proposed a model to effectively address security risks stemming from university network configuration, despite not considering other essential elements of information security, including policies, mobile device management, physical security measures, and employee education on information risks. Yilmaz and Yalman (2016) highlights that universities can improve their information security by implementing precautions, providing training for secure application development, and prioritizing data categorization and encryption.

3. MATERIALS AND METHODS

3.1. Research Design and Approach

Considering the limited research in the area of the selected topic, the current study adopted an exploratory research design and leveraged quantitative and qualitative approaches. The exploratory research design enables the researcher to gain a deeper understanding of the issue (Kumar, 2015). Online and offline survey questions were distributed by email and in person, respectively, to collect quantitative data. Following rigorous assessment of different International ISRM Frameworks, Standards, and Best Practices (Al-Ahmad & Mohammed, 2015; International Telecommunication Union [ITU], 2020; Nagar, 2018; National Institute of Standards and Technology [NIST], 2024; PCI Security Standards Council, 2008; Priest, 1988; SANS Institute, 2016; The British Standards Institution, n.d.; U.S. Department of Health and Human Services, 2025) the study formulated survey questionnaires considering organizational, people, physical, and technological controls. The qualitative data were gathered from a thesis, a recent journal publication, international frameworks, and an interview with information and communication technology (ICT) directors.

3.2. Study Population and Sampling Techniques

The study employed a purposive sampling technique by selecting cases that would help to comprehend the current status of information security in Ethiopia's HEIs, as well as enabling the researcher to select respondents with information security awareness and domain expertise. Purposive sampling is a form of non-probability sampling in which researchers rely on their judgment when choosing elements/members of the population to participate in their study. It is also known as judgment sampling (Campbell et al., 2020). The sample size was determined based on the Raosoft online sample size calculator (Raosoft Inc., Seattle, WA, USA) and the recommended sample size was 258 respondents out of the total population of 5,534 for sufficient generalization.

3.3. Data Collection Procedures

The study employed online survey questionnaires that were prepared using Google Cloud Forms (Google, Mountain View, CA, USA) and used printed or paper-based surveys. The data collection instrument underwent multiple stages of validation to guarantee both data accuracy and reliability. The first validation stage involved a pilot test with 15 participants from two public universities. The research team used the pilot test to find unclear language in the items, to improve the order of the questions, and to calculate the time needed to finish the survey. The pilot group feedback helped researchers enhance the questionnaire clarity and decrease response bias. The revised questionnaire underwent an expert review for content validity during its second stage. Three experts with knowledge in information security and risk management evaluated the items to determine their relevance and their match with ISRM frameworks (ISO/IEC 27005; NIST SP 800-30) and their appropriateness for Ethiopian HEIs. The experts provided feedback, which led to small modifications that improved construct validity. The instrument underwent Cronbach's alpha analysis to test its internal reliability following the completion of the main data collection. The Cronbach's alpha values for the different constructs ranged from 0.78 to 0.86, which falls within the acceptable to good reliability range. The results show that each construct's items measured the specific ISRM dimension consistently. The process included multiple bias mitigation strategies. The study used voluntary participation with anonymity and simple language to prevent confusion among participants. The research targeted participants from various universities and staff positions to reduce selection bias while enhancing generalizability.

The printed questionnaires were distributed among respondents who did not have access to the Internet, as their participation was crucial for the study. Those questionnaires were distributed to ICT professionals and academic staff of Wolaita Sodo University (WSU), Arba Minch University (AMU), Wachemo University (WCU), and Werabe University (WRU). In addition, four ICT directors of those institutions were interviewed to collect detailed qualitative facts. The study conducted a rigorous review and analysis of relevant scholarly literature, including journal articles, research theses, dissertations, and project reports, to look for open issues and best practices.

The researcher underscored the imperative to uphold ethical considerations throughout all process stages, including data gathering and subsequent post-collection endeavors (Cacciattolo, 2015). Upon completion of data collection, the researcher followed strict protocols for the secure storage, retention, and destruction of the collected data, following institutional and regulatory requirements.

3.4. Information Security Risk Management Framework Validations

The proposed 9-step ISRM framework was validated by four domain experts, including two academics specializing in information security and two practitioners from higher education IT departments. Both the thesis supervisors and the examining committees evaluated and gave encouraging comments about the ISRM during the Master of Science (MSC) thesis defense.

4. RESEARCH RESULTS

Microsoft Excel 2016 (Microsoft, Redmond, WA, USA) was used for data analysis. According to the data analysis, 77% of the respondents were male, and 23% were female. The respondents' age range was primarily between 30 and 40 years old, with 64% of them falling into this age range, 27% into the 20-30 age group, and the remaining 9% into the >40 age group. Of the respondents, 47% held a master's degree, 37% held a first degree, and the remaining 8% held a doctorate (Ph. D.) or diploma. Respondents with 5-10 years of experience made up the majority (47.9%), followed by those with >10 years (28.2%), 3-5 years (18.2%), and 0-3 years (5.6%).

To identify existing gaps, best practices, and potential avenues for improvement, the study thoroughly evaluated ISRM within the framework of HEIs in Ethiopia. The study examined well-known international standards and practices from four distinct angles—organizational, human, physical, and technological controls to accomplish these goals (see Sections 4.1 to 4.4 below).

4.1. Responses from Academic Staff Members on Organizational Controls Perspective

Organizational Controls encompass assessment results regarding information security policies, classification and handling of sensitive data, and understanding of any applicable legal data protection laws and privacy regulations, as shown in Table 1.

As indicated in Table 1, most respondents (48%) said "I don't know" in response to the presence of institutional information security policy, indicating significant ambiguity across academic institutions. "No" responses comprised 38%, implying awareness of policy absence within these settings. Affirmative "yes" responses were the smallest segment at 19%. This distribution reveals variable knowledge levels and potential gaps in policy development, communication, and familiarity within academic institutions.

The data analysis results regarding familiarity with protocols surrounding proper data classification, handling,

Table 1. Study participants' response regarding organizational controls

Organizational controls	Questions	Yes (%)	No (%)	Not sure (%)
Information security policies	Does your institution have an approved information security policy that has been published, communicated to relevant staff, and acknowledged by them?	19	38	48
Classification and handling of sensitive data	Do you, as academic staff, have familiarity with protocols surrounding proper data classification, handling, and access control in your institution?	85	15	0
Understanding of any applicable legal data protection laws & privacy regulations	Do you, as academic staff, possess a basic understanding of the legal, regulatory, and contractual requirements—such as data protection and privacy laws—that govern information security at your institution?	66	11	24

HEIs, higher education institutions; ISO, International Organization for Standardization.

and access control show that 15% responded "no," while 85% provided "yes" responses. This distribution suggests a strong comprehension among the academic community of the significance of these information security best practices within the higher education setting.

The data analysis results regarding academic staff awareness of legal, regulatory, and contractual requirements related to information security within their institution reveal varying levels of understanding, with 66% showing awareness, 24% expressing uncertainty, and 11% indicating a lack of awareness. This visual representation offers valuable insights into the knowledge landscape of information security within the academic community.

4.2. Responses from Academic Staff Members on People Controls Perspective

People Controls encompasses assessment results regarding information security responsibilities, reporting of suspected information security incidents, an independent information security policy review team, information security (awareness, education, and training), knowledge about common social engineering attack techniques, formalized disciplinary processes, information security policies for remote workers, and signing of a non-disclosure agreement, as shown in Table 2.

The data analysis results in Table 2 indicate that 17% of respondents do not have explicit information security duties outlined in their roles, while 83% reported the presence of such responsibilities. This disparity underscores the varying levels of focus on information security within academic staff responsibilities, emphasizing the importance of enhancing security measures in educational settings.

With an increasing number of cybersecurity incidents and skills shortage in attack identification and prevention, it is vital to assess the knowledge gap between cybersecurity education and industrial/institutional needs (Catal et al., 2023). In this respect, our study assessed whether academic staff had undergone specific training to facilitate the prompt reporting of observed or suspected incidents through designated channels. It is noteworthy that 18% of academic staff members reported receiving such tar-

Table 2. Study participants' response regarding people controls

People controls	Questions	Yes (%)	No (%)	Not sure (%)
Information security responsibilities	In your job description as academic staff, do your written responsibilities explicitly include information security responsibilities?	83	17	0
Reporting of suspected information security incidents	Have you, as academic staff, received training that specifically covers the establishment of a system for personnel to promptly report observed or suspected information security incidents through the appropriate channels?	82	18	0
An independent information security policy review team	Are you aware of an independent reviewer in your institution who ensures that information security is implemented and operated in accordance with the organization's information security policy, topic-specific policies, rules, and standards?	10	65	25
Information security (awareness, education, and training)	Did you receive any information security awareness, education, and training from information and communication technology staff as an academic staff member?	17	83	0
Knowledge about common social engineering attack techniques	As academic staff, are you knowledgeable about common social engineering attack techniques, such as phishing emails?	64	36	0
Formalized disciplinary process	Is there a formalized disciplinary process in place that is communicated to academic staff regarding the actions to be taken against personnel and other relevant interested parties who have committed an information security policy violation in your institution?	19	57	24
Information security policy for remote workers	Is there a policy in place that mandates the implementation of security measures when personnel are working remotely to protect information accessed, processed, or stored outside the university's premises?	15	32	53
Signing of non-disclosure agreements	As academic staff, are you required to sign a confidentiality or non-disclosure agreement as part of your initial terms and conditions of employment or through an internal memo?	22	46	32

 https://doi.org/10.1633/JISTaP.2026.14.2.1

geted training, indicating a proactive approach to incident reporting within this subset. However, the predominant response of 82% of academic staff lacking this specialized training reveals a notable gap in preparedness and awareness regarding the critical process of reporting information security incidents. This disparity underscores the importance of enhancing training initiatives to empower academic staff with the requisite skills and knowledge to effectively navigate and report security incidents through the appropriate channels in educational settings.

The data analysis results reveal that 10% of academic staff members were cognizant of the existence of an independent reviewer to ensure the implementation and operation of information security in alignment with the organization's policies, topic-specific guidelines, rules, and standards. In comparison, 65% were not aware, and 25% responded with uncertainty. This data underscores potential gaps in communication and transparency regarding information security oversight mechanisms within academic institutions.

It is apparent that a minority of academic staff members, specifically 17%, have participated in information security awareness, education, or training sessions conducted by ICT staff. In contrast, the majority of 83% of respondents have not taken advantage of such opportunities to enhance their knowledge in information security. The data highlights a clear opportunity for HEIs to prioritize and strengthen information security initiatives, thereby better equipping their staff to safeguard sensitive data.

The findings reveal that a majority, constituting 64% of respondents, expressed knowledge of common social engineering techniques, including phishing emails. In contrast, 36% of participants indicated a lack of awareness in this area. This underscores the importance of enhancing awareness and training programs on social engineering among academic staff to fortify cybersecurity measures effectively.

The findings reveal that 19% of respondents confirmed the existence of a formalized disciplinary process for information security policy violations, while a significant portion, comprising 57%, expressed uncertainty about its implementation. Additionally, 24% of participants indicated the absence of a formalized disciplinary procedure for addressing information security policy breaches. The data suggests a critical need for academic institutions to improve their information security governance and communication strategies. The lack of clarity and uncertainty among academic staff members regarding disciplinary processes for handling information security policy violations indicates a potential gap in awareness and preparedness.

The data analysis results show that 15% of respondents had a high level of awareness by acknowledging the presence of a policy that dictates the implementation of security protocols to safeguard information accessed, processed, or stored outside the university's physical confines. In contrast, a considerable majority, comprising 53%, expressed uncertainty or a lack of clarity regarding the existence of such a policy, indicating potential gaps in communication or awareness within the academic community. Furthermore, 32% of participants explicitly stated the absence of a formal mandate requiring the adoption of security measures during remote work activities, highlighting areas where organizational policies may need enhancement. These findings emphasize the critical importance of fostering a culture of information security and promoting clear guidelines for maintaining data confidentiality in diverse work settings, especially those beyond the traditional campus environment.

The data analysis results regarding the obligation to sign a confidentiality or non-disclosure agreement reveal that 46.3% of academic staff members indicated that they are not required to sign such agreements, signaling potential variations in confidentiality protocols across universities. Additionally, 32.1% expressed uncertainty about this requirement, suggesting a need for enhanced communication and clarity regarding confidentiality expectations. On the other hand, 21.6% of respondents affirmed the necessity of signing confidentiality agreements, highlighting a subset of staff members who are subject to such obligations.

4.3. Responses from Academic Staff Members on Physical Controls Perspective

Physical Controls encompass respondents' understanding of the physical security measures and clear procedures for disposing of physical documents, as shown in Table 3.

As shown in Table 3, 88% of academic staff members understand the importance of physical security measures, such as securing offices and reporting suspicious activities. However, 12% of staff members indicated a lack of comprehension in this area. These findings highlight the significance of promoting awareness and adherence to physical security protocols among academic staff to enhance workplace safety and protect sensitive information.

Our study unveils the responses of academic staff members concerning the existence of a clear policy or procedure for managing and disposing of sensitive or con-

Table 3. Study participants' response regarding physical controls

Physical controls	Questions	Yes (%)	No (%)	Not sure (%)
Understanding of physical security measures	Do you understand the importance of physical security measures, including locking offices, securing sensitive documents, and promptly reporting any suspicious activities or individuals?	88	12	0
Clear procedure for disposing of physical documents	Is there a clear policy or a procedure for handling and disposing of sensitive or confidential physical documents or media in your institution?	4	42	54

fidential physical documents or media within their institution. The percentages corresponding to the responses are delineated as follows: 4% indicated the presence of such a policy, 54% expressed uncertainty regarding its existence, and 42% confirmed the absence of a defined protocol for handling confidential physical information. The findings highlight a potential need for improved communication, training, and implementation of structured guidelines for managing confidential information in physical formats. Establishing clear policies and procedures in this area is essential to ensure data security, compliance, and risk mitigation within academic institutions.

4.4. Responses from Information and Communication Technology Staff Members on Technological Controls Perspective

Technological Controls ensures the presence of information security compromises or incidents; inventory teams for critical IT infrastructure; certified information security professionals; backup systems; up-to-date and licensed anti-malware software; patch management; BYOD policy; know-how regarding an emerging security risks and new technology trends; third party software risks; approved business continuity plans; encryption techniques; fraudulent website blocking; expertise in fixing hardware or software issue; a standardized information security framework; regular penetration testing; and evaluation of information security control effectiveness, as shown in Table 4.

The ICT personnel were asked about the occurrence of information security breaches within their institutional frameworks in recent years. The corresponding percentages for each response category are delineated as follows: Yes - 44.44%, No - 31.11%, and I don't know - 24.44%. These quantitative metrics offer valuable insights into the frequency of security incidents and the level of cognizance among ICT professionals within the surveyed academic institutions. The findings underscore the need for continual vigilance and proactive measures to strengthen information security practices in the academic sector.

The research inquiry targets ICT personnel in selected universities regarding the establishment of a comprehensive inventory or registry specifically tailored for pivotal assets within each cybersecurity system managed by their ICT directorates. The data breakdown illustrates that 46% of respondents acknowledge the implementation of such a system, while 30% negate its existence, and 24% remain uncertain about the presence of an organized inventory or registry for these critical assets. This indicates potential variations in approaches to asset management and underscores the importance of further potential enhancement of asset management protocols within academic ICT directorates.

The study assessed the availability of designated information security staff in ICT directorates for managing information security cases. The findings reveal that 9% of respondents affirm the existence of such staff, while a majority of 78% indicates a lack of designated personnel for this role. Additionally, 13% of respondents express uncertainty regarding the presence of information security staff within the ICT directorate. The findings imply a notable gap in the allocation of designated information security staff within ICT directorates of selected universities.

The question was posed to the ICT staff of the selected universities regarding the presence of certified information security professionals within the ICT directorate of their respective institutions. The highest percentage (57%) of respondents signaled the lack of certified information security professionals. Subsequently, 30% expressed uncertainty, while only 13% confirmed certified information security professionals. Overall, these implications highlight areas for improvement in strengthening information security capabilities within academic settings to effectively protect valuable data assets.

The data obtained from ICT staff at selected universities regarding the presence of a backup system for critical data protection and disaster recovery measures within their institutions indicates that 11% of partici-

Table 4. Study participants' responses regarding technological controls

Technological controls	Questions	Yes (%)	No (%)	Not sure (%)
Information security compromises or incidents	Has your institution ever been compromised by information security issues in the last few years?	44.44	31.11	24.44
Inventory or registry of important cybersecurity assets	Is there a defined inventory or registry maintained for important assets associated with each cybersecurity system within your ICT directorate?	46	30	24
Designated Information Security staff in the ICT directorate	Are there designated information security staff within the ICT directorate who are responsible for handling information security cases?	9	78	13
Certified information security professionals within the ICT directorate	Are there any certified information security professionals within the ICT directorate of your institution?	13	57	30
Backup systems for disaster recovery	Is there a backup system in place to safeguard critical data and facilitate disaster recovery in the event of data loss or system failure in your institution?	11	62	17
The university's up-to-date licensed anti-malware software	Does the university have up-to-date and licensed anti-malware software in place to protect its systems and endpoints from malicious software threats?	13	50	37
Patch management in the university's critical infrastructure	Is there a patch management system in place at the university to ensure that systems and endpoints are regularly updated with the latest security patches and updates?	8	70	22
BYOD policy or framework	Is there a policy or framework in place regarding BYOD at the university?	10	77	13
Emerging security risks and new technology trends	Do you stay updated on emerging security risks and new technology trends?	24	76	0
Specific approaches for the risk associated with third-party software	Does your institution have a specific approach in place to manage information security risks associated with third-party software applications?	50	18	32
Institution-approved business continuity plans	Has the institution developed an approved business continuity plan?	45	16	29
Implementation of encryption in the institution	Has your institution implemented encryption?	40	31	29
Enforcement of specific requirements	Does your ICT directorate have measures in place to enforce specific password requirements for system and account access?	77	23	0
Blocking access to certain types of websites	Does your organization have a practice in place to identify the types of websites to which personnel should or should not have access, and does it consider blocking access to certain types of websites?	68	8	23
Establishment of risk measurement criteria	Does your organization have established risk measurement criteria for assessing and managing ICT risks?	7	83	10
Reliance on service providers for information security risk management	In the context of information security risks, do you rely on service providers for some or your entire IT infrastructure?	61	26	13
Availability of a professional to fix a hardware or software issue	In the event of a hardware or software issue in the data center, are there professionals available to fix it?	92	8	0

ICT, information and communication technology; BYOD, Bring Your Own Devices.

pants affirmed the availability of a backup system, while the majority of 62% stated the absence of such a system. Furthermore, 17% of respondents expressed uncertainty regarding the presence of backup measures in place. This data underscores a concerning trend where a substantial portion of institutions lack adequate backup systems, posing potential risks in data security and disaster preparedness within academic ICT settings.

The responses obtained from ICT staff members regarding the presence of up-to-date and licensed anti-malware software within the university environment indicate that 50% of respondents indicate a lack of up-to-date and licensed anti-malware software. Following closely, 37% expressed uncertainty, while only 13% confirmed the presence of such protective measures. The findings underscore the urgency for proactive measures to strengthen university cybersecurity postures.

The data obtained from the survey of ICT staff in universities regarding the presence of a patch management system reveals that the highest percentage, with 70% of respondents, reported the absence of such a system, indicating a critical gap in cybersecurity practices. Following this, 22% expressed uncertainty about the implementation of a patch management system, highlighting the need for clarity and communication in cybersecurity protocols. Lastly, only 8% confirmed the presence of a patch management system, underscoring the importance of enhancing cybersecurity measures within university ICT departments. These findings emphasize the necessity for universities to prioritize the establishment of effective patch management systems.

The data collected from the survey of ICT staff in universities regarding the existence of a policy or framework concerning BYOD practices reveals that 77% of respondents indicated the absence of a BYOD policy or framework at their institutions. In contrast, 13% expressed uncertainty about the presence of such guidelines, while only 10% confirmed the existence of a BYOD policy. These results underscore the need for universities to focus on developing and implementing clear BYOD policies to effectively manage and regulate personal device usage within academic settings.

The responses of ICT staff from selected universities regarding their practice of staying updated on emerging security risks and new technology trends reveal that 24% of respondents indicated that they stay updated on these aspects, reflecting a proactive approach to knowledge enhancement within the field. Conversely, 76% of respondents reported not staying updated, highlighting a potential gap in awareness and readiness to address evolving security challenges and technological advancements. This data suggests the importance of continuous learning and vigilance in staying abreast of emerging trends for effective ICT management within university settings.

The responses of ICT staff from universities regarding the presence of a specific approach to manage information security risks associated with third-party software applications illustrate that 18% of respondents indicate their institution does not have a specific approach in place for managing these risks. In contrast, 32% of respondents stated that they were unsure if such an approach existed, while 50% confirmed the presence of a defined strategy for handling information security risks related to third-party software applications. This data suggests that a significant majority of universities may need to enhance their measures in addressing security risks associated with third-party software applications.

The responses from ICT staff at universities indicate that 45% have confirmed the presence of an approved business continuity plan, signifying proactive measures towards operational resilience. Conversely, 16% reported a lack of such a plan, suggesting potential vulnerabilities in addressing unforeseen disruptions. The significant percentage of 29% expressing uncertainty underscores the importance of enhancing communication and clarity regarding business continuity strategies within the university's ICT directorate. This data highlights the crucial role of robust continuity planning in ensuring organizational preparedness and mitigating risk in the dynamic landscape of HEIs.

The perspectives of ICT staff from HEIs regarding the implementation of encryption within their organizations reveal that 40% of respondents confirmed the presence of encryption measures in place, indicating a proactive stance towards data security and confidentiality. Alternatively, 31% of respondents reported that their institution has not implemented encryption, highlighting a potential gap in safeguarding sensitive information. Additionally, 29% of respondents expressed uncertainty about the status of encryption implementation, underscoring the need for clarity and awareness regarding data protection strategies within university ICT environments. This data highlights the importance of robust encryption practices in enhancing cybersecurity measures and mitigating risks in higher education settings.

The responses from ICT staff regarding the existence of measures within their ICT directorate to enforce specific password requirements for system and account access

 https://doi.org/10.1633/JISTaP.2026.14.2.1

reveal that 77% of respondents confirmed the presence of such measures, indicating a proactive approach to enhancing security protocols. However, 23% of respondents indicated the absence of enforced password requirements, suggesting potential vulnerabilities in access control mechanisms. This data highlights the importance of robust password policies in safeguarding system integrity and data confidentiality within ICT environments, emphasizing the need for comprehensive security measures to mitigate risks effectively.

The responses obtained from ICT staff regarding the presence of organizational practices to identify permissible and restricted website categories for personnel access, including the consideration of blocking access to specific websites, indicate that 68% of respondents affirmed the existence of such practices. In contrast, 8% of respondents stated that their organization does not have such practices in place. Moreover, 23% of respondents expressed uncertainty on this matter, emphasizing the need for clearer communication and implementation of website access policies within organizational frameworks. These findings underscore the significance of establishing robust protocols to regulate website access, mitigate risks, and maintain a secure digital environment within the organization.

The responses from ICT directorate staff regarding the presence of established risk measurement criteria for assessing and managing ICT risks within their organizations reveal that 83% of respondents indicated the absence of such criteria, while 7% confirmed the existence of established risk measurement criteria. Additionally, 10% of respondents expressed uncertainty on this matter, emphasizing the importance of clarity and alignment in risk assessment frameworks within organizational ICT contexts. These insights underscore the critical importance of implementing effective risk measurement criteria to bolster risk management practices and fortify ICT resilience in organizational contexts.

The insights from ICT staff regarding their reliance on service providers for managing some or all aspects of their IT infrastructure within the realm of information security risks indicate that a majority of respondents, accounting for 61%, acknowledge leveraging service providers, reflecting a strategic outsourcing strategy for IT infrastructure management. On the contrary, 26% of respondents indicated a self-reliant approach, preferring internal control over their IT infrastructure without external service provider involvement. Furthermore, 13% of respondents expressed uncertainty regarding their reliance on service providers, emphasizing the necessity for a deeper understanding of the implications of such dependencies on information security risks. These findings underscore the significance of assessing the strategic implications of outsourcing IT infrastructure on ISRM practices within organizational contexts.

The responses provided by ICT staff concerning the availability of professionals to address hardware or software issues within the data center setting reveal that 92% of respondents acknowledge the presence of skilled professionals poised to resolve technical issues, signifying a proactive stance towards expedient problem resolution. Conversely, 8% of respondents indicate a dearth of professionals available for troubleshooting, hinting at a potential insufficiency in technical support within the data center milieu. These findings underscore the importance of having skilled professionals on hand to ensure efficient maintenance and troubleshooting of hardware and software issues in data center operations, thereby enhancing overall operational resilience and continuity.

The study reveals significant insights into HEIs in Ethiopia regarding the adoption of information security standards, best practices, and frameworks by AMU, WSU, WRU, and WCU. Firstly, WRU emerges as the frontrunner in embracing the "ISO 27001" standard, showcasing the highest adoption rate at 14%. Conversely, AMU exhibits a notable level of uncertainty, with 14% of responses falling into the "I don't know" category, indicating a potential area of ambiguity or lack of clarity in information security practices. Moreover, WSU and WCU demonstrate a moderate approach to adoption, with the former showing an 8% utilization of "COBIT" and the latter implementing "CISCO ASA" at a rate of 6%. Both AMU and WSU reveal lower levels of utilization in categories such as "no framework/standard," "PCI DSS," and "HIPAA," each registering at 2% or below. Overall, the findings underscore the importance of continued exploration into the factors influencing the adoption patterns of information security frameworks within academic institutions. By addressing areas of uncertainty, enhancing moderate adoption levels, and improving low utilization rates, universities can strengthen their information security posture and better protect sensitive data assets against evolving threats and vulnerabilities.

We observed responses from ICT staff at specific universities regarding the frequency of penetration testing to evaluate the security posture of systems and networks. The data showcases that a significant majority of 86% of respondents stated never engaging in penetration testing activities. Following this, 9% of participants indicated oc-

casional testing, while a smaller percentage of 6% reported conducting penetration testing regularly. This breakdown underscores a notable gap in consistent security evaluation practices, with occasional penetration testing being less common for the majority.

We observed responses from ICT staff regarding the frequency of evaluating the effectiveness of information security controls in the university context. The analysis indicates that 78% of respondents reported that these evaluations are never conducted, suggesting a potential area for improvement in assessing and strengthening security measures. In contrast, 9% of respondents stated that evaluations are regularly carried out, reflecting a proactive approach to monitoring and enhancing information security practices. Additionally, 13% of respondents mentioned that evaluations occur occasionally, indicating a moderate level of attention towards assessing security controls. These findings emphasize the significance of consistent and thorough evaluations to uphold the robustness of information security measures within the university.

4.5. A Comparative Presentation of Each Higher Education Institutions's Perspectives on Organizational, People, Physical, and Technological Controls

The comprehensive analysis in Table 5 unveils a nuanced picture of the information security landscape at AMU, WSU, WCU, and WRU. Each institution showcases distinct strengths and weaknesses across organization controls, people control, physical controls, and technological controls.

Organization controls: AMU and WCU are advancing in data classification, while WSU demonstrated an awareness of legal compliance. However, the communication of information security policies to staff is a concern for AMU and WCU. WSU is also facing challenges in effectively communicating security policies to staff and understanding sensitive data classification. WRU is struggling with comprehending data classification and legal requirements, and lacks a universally accepted security policy.

People control: AMU and WCU have well-informed academic staff regarding phishing emails. However, a significant weakness is the lack of delineated information security responsibilities in the job descriptions of their academic staff. Additionally, there is a noticeable absence of an independent security compliance reviewer, incident reporting training, ICT-led security education, breach disciplinary procedures, remote work security protocols, and confidentiality agreements at the onset of employment. On the other hand, WSU and WRU lack awareness of phishing emails and do not specify information security responsibilities in job descriptions. These institutions also do not have an independent security compliance reviewer, incident reporting training, ICT-led security education, formal breach disciplinary procedures, remote work security protocols, and confidentiality agreements established at the start of employment.

Physical controls: AMU, WSU, and WCU emphasize physical security measures such as office locking and robust controls in the data center, including environmental and access control measures, and reporting suspicious activities. However, AMU lacks clear protocols for handling sensitive documents and video surveillance systems. WSU faces weaknesses in managing sensitive documents, video surveillance, redundancy, and disaster recovery systems. WRU demonstrates shortcomings in implementing physical security measures, particularly office locking and data center controls, as evidenced by deficiencies in perimeter security, video surveillance, redundancy systems, environmental controls, and access mechanisms.

Technological controls: The investigation indicates that all universities have developed definitive inventories of essential assets within their cybersecurity frameworks, institute-specific password policies, and clearly defined authorized website access for personnel. Nevertheless, a common vulnerability among these institutions is the lack of dedicated information security staff and certified experts. AMU is deficient in established risk assessment criteria for the management of ICT risks. WSU is particularly lacking in the evaluation of information security control efficacy, the implementation of encryption, system updates for security patches, and BYOD policy. WCU encountered a shortage of certified security personnel, dedicated ICT security staff, faced difficulties in penetration testing, and had issues with data backup systems. WRU is missing critical security measures such as penetration testing and anti-malware software.

5. DISCUSSION ON KEY RESEARCH FINDINGS

5.1. Organizational Controls Perspective

Despite most academic staff having familiarity with protocols surrounding proper data classification, handling, and access control in their institution, as well as having a basic understanding of applicable legal, regulatory (such as data protection laws and privacy regulations), or contractual requirements related to information security in their institution, they were not sure about the pres-

 https://doi.org/10.1633/JISTaP.2026.14.2.1

Table 5. A comparative presentation of each HEI's perspectives on organizational, people, physical, and technological controls

Thematic areas	University strengths and weaknesses			
	AMU	WSU	WCU	WRU
Organizational controls perspective	While the university has made progress in data classification, there are gaps in legal compliance and ineffective communication of its information security policy to staff members	The university staff demonstrates awareness of legal requirements but lacks effective communication of the information security policy to staff and understanding of sensitive data classification	The staff at the university understands data classification levels but lacks awareness of legal requirements for information security, and the institution also lacks a published security policy for staff	University academic staff exhibit a deficiency in comprehending data classification and legal requirements, alongside the absence of a universally acknowledged security policy within the institution
People controls perspective	University academic staff are aware of social engineering techniques but lack independent security policy oversight, structured incident reporting, robust remote work security measures, confidentiality agreements in employment terms, and comprehensive information security training	The study revealed that the university academic staff lack awareness of phishing emails and information security responsibilities in job descriptions. The institution lacks an independent security compliance reviewer, incident reporting training, ICT-led security education, disciplinary processes for breaches, a remote work security policy, and confidentiality agreements at employment commencement	The academic staff at the university are aware of phishing emails but lack information security responsibilities in job descriptions. The institution lacks an independent security compliance reviewer, incident reporting training, ICT-led security education, breach disciplinary procedures, remote work security protocols, and confidentiality agreements at employment start	The university academic staff lack awareness of phishing emails and information security responsibilities in job descriptions, while the institution lacks an independent security compliance reviewer, incident reporting training, ICT-led security education, formal breach disciplinary procedures, remote work security protocols, and confidentiality agreements at the start of employment
Physical controls perspective	The university prioritizes physical security measures like office locking and robust controls in the data center, such as perimeter security, redundancy systems, environmental controls, and access control mechanisms, and reporting suspicious activities, but lacks clear protocols for sensitive documents and video surveillance systems	The university recognizes the importance of physical security measures, including office locking, safeguarding documents, and reporting suspicious activities. Weaknesses are apparent in handling sensitive documents, video surveillance, redundancy, and disaster recovery systems	The university emphasizes physical security measures like office locking, data center controls, perimeter security, redundancy systems, environmental controls, and access mechanisms. Clearer protocols for sensitive documents and video surveillance implementation have been put in place	The university's implementation of physical security measures, particularly office locking and controls within the data center, is not given due priority. This is evidenced by shortcomings in perimeter security, video surveillance, redundancy systems, environmental controls, and access mechanisms
Technological controls perspective	The university has established a clear inventory of crucial assets linked to each cybersecurity system, enforces specific password protocols for system and account entry, determines authorized and unauthorized website access for personnel, and has implemented encryption measures. Nevertheless, there is a notable absence of dedicated information security personnel, certified professionals in the field, and the establishment of risk measurement criteria or assessing and managing (ICT) risks	The research findings indicate that the university has successfully enforced specific password criteria for system and account access, and a structured inventory for critical assets related to each cybersecurity system. However, there is a notable absence of assessment of information security control efficiency, encryption implementation, regular system updates for security patches, and an established policy for BYOD at the university	The university displays proactive measures in addressing security risks and technology advancements, enforcing password protocols, managing website access, and providing expertise for data center maintenance. Nevertheless, there are shortcomings in certified security personnel, dedicated ICT security staff, conducting penetration testing, and establishing backup systems for data protection	The university is diligent in addressing emerging security risks and technology trends, enforcing password protocols, and managing website access. Yet, there are deficiencies in designated information security staff, certified professionals, asset inventory for cybersecurity, and essential security measures like penetration testing and anti-malware software

HEI, higher education institution; AMU, Arba Minch University; WSU, Wolaita Soddo University; WCU, Wachemo University; WRU, Werabe University; ICT, information and communication technology; BYOD, Bring Your Own Devices.

ence of information security policies in their institutions. These findings indicate the importance of establishing and communicating a proper information security policy with each academic staff member for appropriate data classification, handling, and access control. Petersen (2013) stated that colleges and HEIs must conform to different legislative requirements at the federal/national, regional, and local levels when dealing with the handling of different public records. These institutions vary in size, financial resources, and human capital; they are often required to concentrate on addressing different risks or priorities. Regulatory and compliance requirements encompass notifying data breaches and reporting laws for public records requests and personally identifiable information.

5.2. People Controls Perspective

Despite most academic staff indicating the presence of written responsibilities explicitly including information security responsibilities in their job description, being aware of reporting of suspected information security incidents, and being knowledgeable about common social engineering attack techniques like phishing emails, they did not receive any information security awareness, education, or training from ICT staff. They further indicate a lack of formalized disciplinary processes when information security policy is violated, they were not sure about the presence of information security policies for remote workers, and they indicate a lack of signing non-disclosure agreements in their institution.

The results show how crucial it is to have an independent information security policy review team in order to maintain the current information security policy, its implementation, and its operation.

The ICT staff of each institution is supposed to provide regular information security awareness, education, and training to improve the academic staff's security hygiene. All HEIs are expected to ensure that each employee signs a non-disclosure agreement to safeguard the privacy and security of sensitive data, and they are expected to implement formalized disciplinary processes for information security policy violations by internal and remote workers.

5.3. Physical Controls Perspective

Despite most academic staff understanding the importance of physical security measures, including locking offices, securing sensitive documents, and promptly reporting any suspicious activities or individuals, they indicate a lack of clear policy and procedures for disposing of physical documents in their institutions. These findings show the importance of having a clear policy and procedure in each institution for disposing of physical documents or documents in printed form to prevent information leakage.

Even though most ICT employees report having inventories for critical IT infrastructure, knowing how to deal with third-party software risks, confirming the existence of approved business continuity plans, encryption techniques, confirming the enforcement of access control policies, practicing blocking malicious websites, and confirming the availability of professionals to fix hardware or software issues, the majority of ICT employees report that there have been compromised information security issues in the past few years, and that their ICT directorate lacks certified information security professionals, patch management, BYOD policies, and regular backup systems in their organizations. There is a lack of formal measuring standards for evaluating and controlling ICT risks and penetration testing. Most ICT staff admitted to not keeping up with new developments in technology and security threats.

5.4. Technological Controls Perspective

The most productive cybersecurity professionals can outperform the less experienced graduates in the field. Graduates with expertise in cybersecurity positions can assist institutions and nations in promptly addressing cybersecurity issues (National Research Council, 2013). In the early days, the need for information security experts have been met with employees who are trained in related fields like computer science, information science, software engineering, and more while in recent years, some HEIs have begun to incorporate cybersecurity courses as part of their education curriculum to tackle the shortage of experts in the field (Catal et al., 2023). Considering the aforementioned modern practices, HEIs in Ethiopia are supposed to produce or recruit certified/skilled information security professionals within their ICT directorates to promptly address the shortage of information security experts or the evolving cybersecurity-related issues as well, and have harmonized guidelines for integrating technology, people, and policy/procedures to reduce security incidents. Mobile devices are personal devices that can pose a risk to any institution. In this regard, HEIs are supposed to enforce BYOD policies for encryption of valuable data stored in mobile devices and remotely wipe out data when those devices are lost to prevent sensitive information leakage (Adane, 2020; Grajek, 2015; Petersen, 2013; Yousif Yaseen, 2022).

One of the most valuable resources for universities is information or data, which needs to be safeguarded against security breaches (Joshi & Singh, 2017). The majority of reported breaches in higher education are classified as hacking or malware. These breaches occurred when an outsider used malware, spyware, or direct access to obtain records. Accidental disclosure of private data to an undesired recipient by fax or email, or accidentally made publicly available on a website, as well as the loss of a portable device, such as a stolen or misplaced laptop or memory device, were other reported breaches (Grama, 2014). Malware can occur when an unauthorized piece of software is placed on a user's PC or a higher education server, limiting access and/or resulting in a system crash. Malware comes in many forms, such as worms, viruses, ransomware, and adware (Readiness and Emergency Management for Schools Technical Assistance Center, 2017). Careful monitoring and regular assessment of risks could help HEIs in managing voluminous network traffic flows and the associated vulnerabilities (Grajek, 2015). In this respect, HEIs in Ethiopia are expected to use up-to-date and licensed anti-malware software, perform patch management, implement and practice regular backups of valuable data in the institutions, encourage staff to stay updated regarding emerging security risks and new technology trends, and develop a risk measurement framework for assessing and managing ICT risks.

6. THE PROPOSED COMPREHENSIVE INFORMATION SECURITY RISK MANAGEMENT FRAMEWORK

Based on the findings, our study introduces a novel framework for assessing, protecting against, and preventing information security risks within the context of universities. It delineates a systematic approach to identifying risks associated with critical assets. The internal and external components of the proposed framework are presented as follows.

The study suggests nine (9) steps for implementing the internal components of the proposed framework.

6.1. Step 1 - Establish Risk Measurement Criteria

During the initial phase, key stakeholders, including the head of the ICT directorate, the head of the academic bureau, the head of finance, and university staff, collaborate to set benchmarks for assessing risk impact based on the university's mission and business objectives. The impact areas considered will encompass reputation and customer confidence, financial aspects, productivity, safety and health, as well as potential fines and penalties. Through thorough discussions and analysis, specific criteria for measuring risks will be established by prioritizing the impact areas that can affect the university's mission and objectives. The stakeholders shall fill in the blanks in the criteria worksheet to make them meaningful to the university. These risk measurement criteria will outline the levels of impact—high, medium, and low—enabling the university to effectively evaluate and address risks in alignment with its strategic goals and values.

6.2. Step 2 - Develop an Information Asset Profile

In this phase, the process commences with the establishment of university asset profiles. These profiles serve as detailed representations of each information asset, delineating their unique characteristics, qualities, features, and intrinsic value. The criteria for identifying critical assets encompass their significance to the university, active utilization in daily operational processes, and the potential impact on impeding the university's ability to fulfill its objectives and mission if lost. Each asset's profile is meticulously captured on a dedicated worksheet, as exemplified in Table 6, to provide a structured framework for informed decision-making and proactive risk mitigation strategies.

6.3. Step 3 - Identify Information Asset Containers

In this phase, the emphasis lies on identifying the containers in which the university's information assets are stored, processed, and controlled.

Technical containers: These containers encompass the hardware and software elements that fall within the organization's jurisdiction but also extend beyond its confines. They include essential IT infrastructure components like servers, databases, and networks, which are crucial for information management.

Physical containers: Physical containers denote the tangible locations where physical documents and assets are housed, such as filing systems, secure rooms, and external storage sites. These spaces, both within and outside the organization, store physical information resources securely.

People containers: People containers involve individuals with insights into the organization's information assets, both internally and externally. This category comprises employees, contractors, vendors, and other stakeholders who interact with and possess knowledge about the organization's information landscape.

Table 6. Establishing HEI critical information asset profile

Information asset	Unique features and qualities	Characteristics	Value
Student records	Personal information, academic history, enrollment status	Sensitive, confidential, regulatory compliance	Critical for academic progress and records
Research data	Experimental results, scholarly publications, intellectual property	Proprietary, research integrity, collaboration	Foundation for scholarly contributions
Financial information	Budgets, grants, transactions, payroll data	Financially sensitive, compliance requirements	Essential for fiscal planning and reporting
Administrative databases	HR records, procurement data, institutional reports	Operational efficiency, administrative support	Facilitates institutional management
Communication networks	Email communications, online collaboration platforms	Real-time communication, data exchange	Enhances collaboration and information sharing
Technology infrastructure	Servers, computers, software applications, databases	Backbone of IT operations, data storage	Supports academic and administrative functions
Physical security	Access control systems, surveillance cameras, security personnel	Safeguards buildings and assets, prevents unauthorized access	Protects physical infrastructure and resources

HEI, higher education institution; HR, human resource.

Table 7. Identification of critical information assets, security threats, and storage locations/containers

Information asset	Threat scenario	Container type
Student records	Data breaches	Technical container
Research data	Cyberattacks	Technical container
Financial information	Insider threats	People containers
Administrative databases	Third-party risks	Technical container
Communication networks	Cyberattacks	Technical container
Technology infrastructure	Physical theft or damage	Physical containers
Physical security	Compliance violations	Physical containers

6.4. Step 4 - Identify Areas of Concern

In Step 4, the process begins by referring back to information asset risk profiles, focusing on threats unique to the university and its operations. Each container is reviewed to list critical assets and identify areas of concern. The goal is not to list every possible threat scenario but to quickly pinpoint situations that could affect university assets. Each document is thoroughly examined to document all relevant concerns on an information asset profile worksheet, including the asset name and a detailed description of the concern.

6.5. Step 5 - Identify Threat Scenarios

In this step, areas of concern are expanded into threat scenarios that further detail the properties of a threat. The threats are assessed by understanding threat scenarios, which involve outlining information assets alongside their corresponding threat scenarios and the containers in which they are stored. A detailed elucidation is presented in Table 7 as follows.

6.6. Step 6 - Identify Risks

In this stage, the primary aim is to document the outcomes for an organization when a threat becomes a reality, thereby concluding the risk assessment process. The assessment of the impact on the university is based on the previously identified threat scenarios and their associated risks. The possible threats to the university's information assets and their corresponding risks are presented in Fig. 1, which enables a detailed examination and understanding of the potential consequences for the university. The evaluation of the consequences to university assets involves analyzing the financial implications of asset loss, hacking incidents, or non-compliance fines with ISRM standards,

 https://doi.org/10.1633/JISTaP.2026.14.2.1

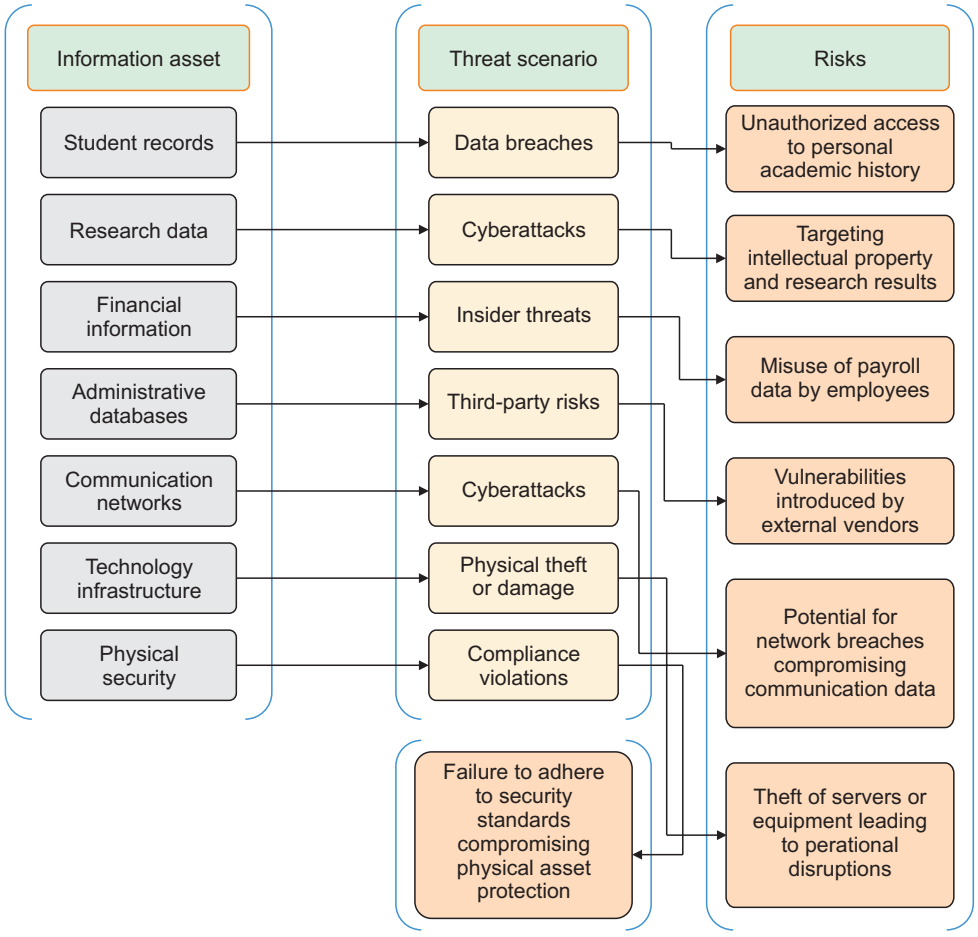


Fig. 1. Risk and security threat identification for information assets.

frameworks, or industry best practices. Understanding the potential costs to the university in these scenarios is essential for effective risk management and strategic decision-making. By assessing these factors, institutions can proactively mitigate risks and safeguard their valuable assets.

6.7. Step 7 - Analyze Risks

The risk analysis starts by referring to the risk measurement criteria created in Step 1, classifying the consequences of each threat on universities according to the criteria of low, moderate, and high. Next, a relative risk score will be calculated, which can be used to analyze risk and help universities determine the right risk strategy. The relative risk score calculation refers to the impact value. The impact value is derived from the risk measurement criteria (Impact area value: Low=1, Medium=2, High=3). Relative risk scores will be calculated and used to analyze risk and help the university to determine the right risk strategy. Each score for each impact area ranking will be multiplied by the impact (Low, Medium, and High) to generate an impact value to guide the focus area. This relative risk score is derived by considering the extent to which the consequence of a risk impacts the organization against the relative importance of the various impact areas, and possibly the probability. In other words, if Financial and Fines, and Legal outcomes are most important to the university, these risks will generate higher scores than risks with equivalent impacts and probabilities in another area. The sample risk analysis is explained in Table 8.

Table 8. Risk score impact sample calculation

Impact area	Ranking	Impact	Impact value
Reputation	2	Medium (2)	4
Financial	5	High (3)	15
Productivity	1	Low (1)	1
Safety and health	3	Low (1)	3
Fines & legal	4	High (3)	12

6.8. Step 8 - Select Mitigation Approach

In Step 8, the final step of the risk management process, the university determines which of the risks it has identified require mitigation and develops a mitigation strategy for those risks. This is accomplished by first prioritizing risks based on their relative risk score. Once risks have been prioritized, mitigation strategies are developed that consider the value of the asset and its security requirements, the containers in which it lives, and the organization's unique operating environment.

Risk acceptance: Evaluate risks that are deemed acceptable and decide to acknowledge them without taking further action.

Risk avoidance: Begin by identifying potential risks and implementing ISO 27001: 2022 controls to avoid them altogether.

Risk reduction: Implement measures to reduce the likelihood and impact of identified risks by adopting ISO 27001: 2022 security controls.

Risk transfer: Transferring certain risks to external parties like insurance providers or third-party vendors to reduce the financial impact on the institution as a result of security incidents.

Risk contingency: Develop contingency plans to prepare for and respond to potential security incidents. The risk mitigation approaches are outlined in Fig. 2.

6.9. Step 9 - Risk Monitoring

The last stage of risk assessment involves the continuous process of identifying, assessing, and managing risks related to information security within an organization. This includes gathering threat intelligence, conducting vulnerability assessments, performing security audits, and monitoring incidents to detect patterns and vulnerabilities. Structured reporting and feedback mechanisms ensure stakeholders are informed and engaged.

The external components of the proposed framework are presented in Figs. 3 and 4 as follows.

Risk communication: exchange of real-time information, advice, and opinions between experts.

Risk documentation: the process of documenting the findings during assessment.

6.10. Validations for the Proposed Information Security Risk Management Framework

A Delphi-style review was conducted to validate the proposed 9-step ISRM framework with four domain experts, including two academics specializing in information security and two practitioners from higher education IT departments. The experts agreed that the framework addressed the unique contextual challenges of Ethiopian HEIs, particularly in balancing formal standards such as

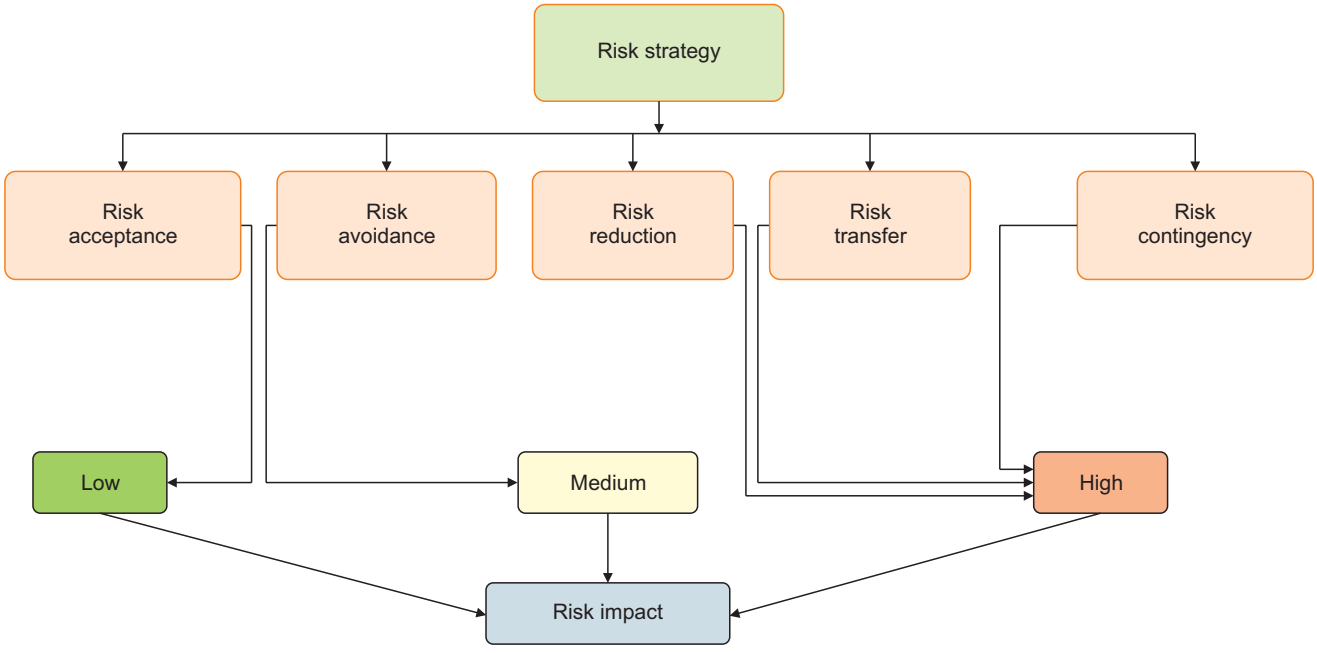


Fig. 2. Risk mitigation approaches.

 https://doi.org/10.1633/JISTaP.2026.14.2.1

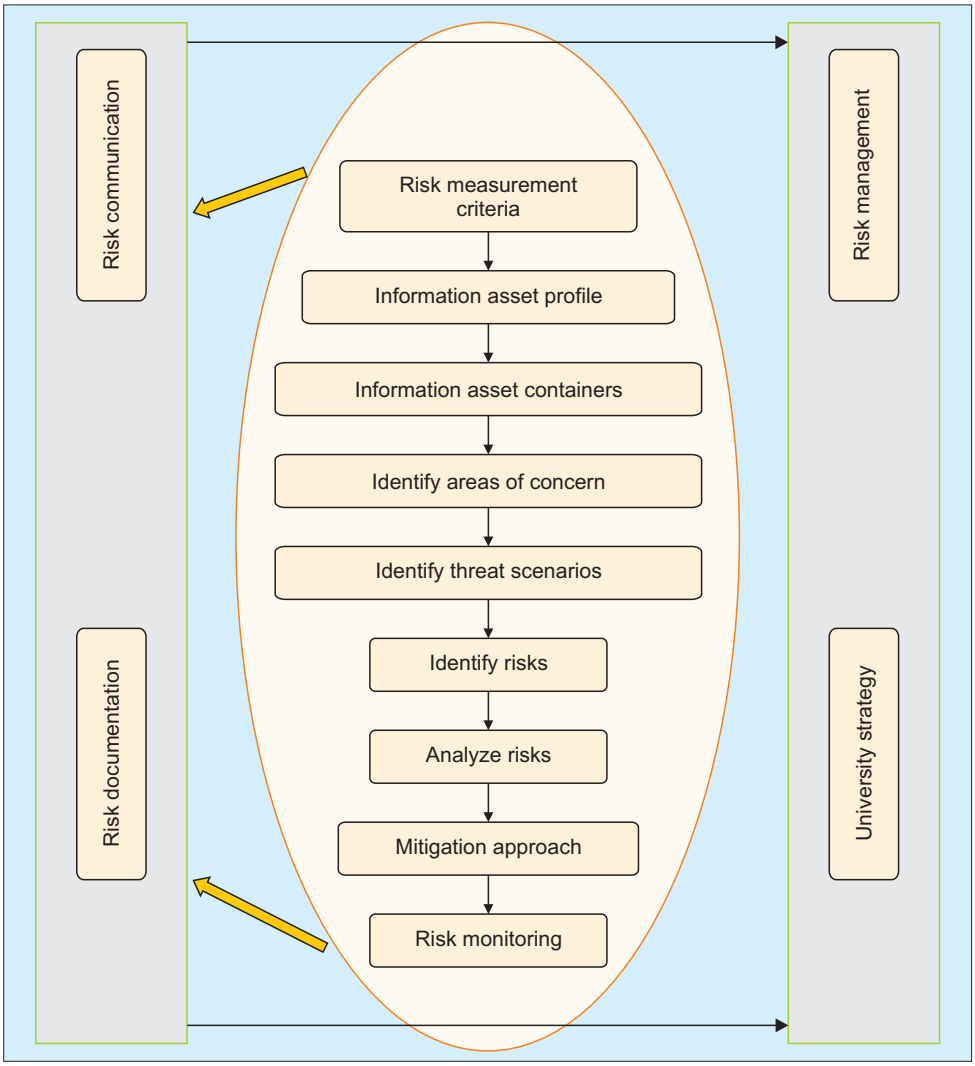


Fig. 3. Proposed comprehensive information security risk management framework.

ISO 27005 (NIST SP 800-30) with resource constraints. Minor suggestions included emphasizing continuous awareness training and clarifying the boundary between Step 6 (Risk Identification) and Step 7 (Risk Analysis). The experts confirmed that the model was relevant, adaptable, and contributed to the ISRM body of knowledge, as indicated in Section 3.4.

7. A COMPARATIVE ANALYSIS OF THE PROPOSED FRAMEWORK VS. INTERNATIONAL STANDARDS/ FRAMEWORKS

The proposed nine-step framework enhances ISRM theory through its explicit inclusion of resource-constraint adaptation within the risk management cycle. The existing ISRM models, including ISO 27001, NIST SP 800-30, and ITU-T X.1055, contain implicit assumptions about sufficient financial, technical, and human resources, which restrict their use in under-resourced settings. The framework implements risk measurement simplification (Step 1) and academic information asset and container profiling (Steps 2-3), and budget-based mitigation strategy prioritization (Step 8) to create a context-aware extension of existing maturity models. The study introduces a fresh theoretical dimension to ISRM theory, which shows that risk management success depends on both strict process adherence and institutional capabilities and flexibility. The research demonstrates how global standards can be transformed into scalable models for diverse institutional contexts through systematic hybridization, which benefits higher education systems in the Global South.

The international standards provide complete structures, yet they require substantial financial and technical

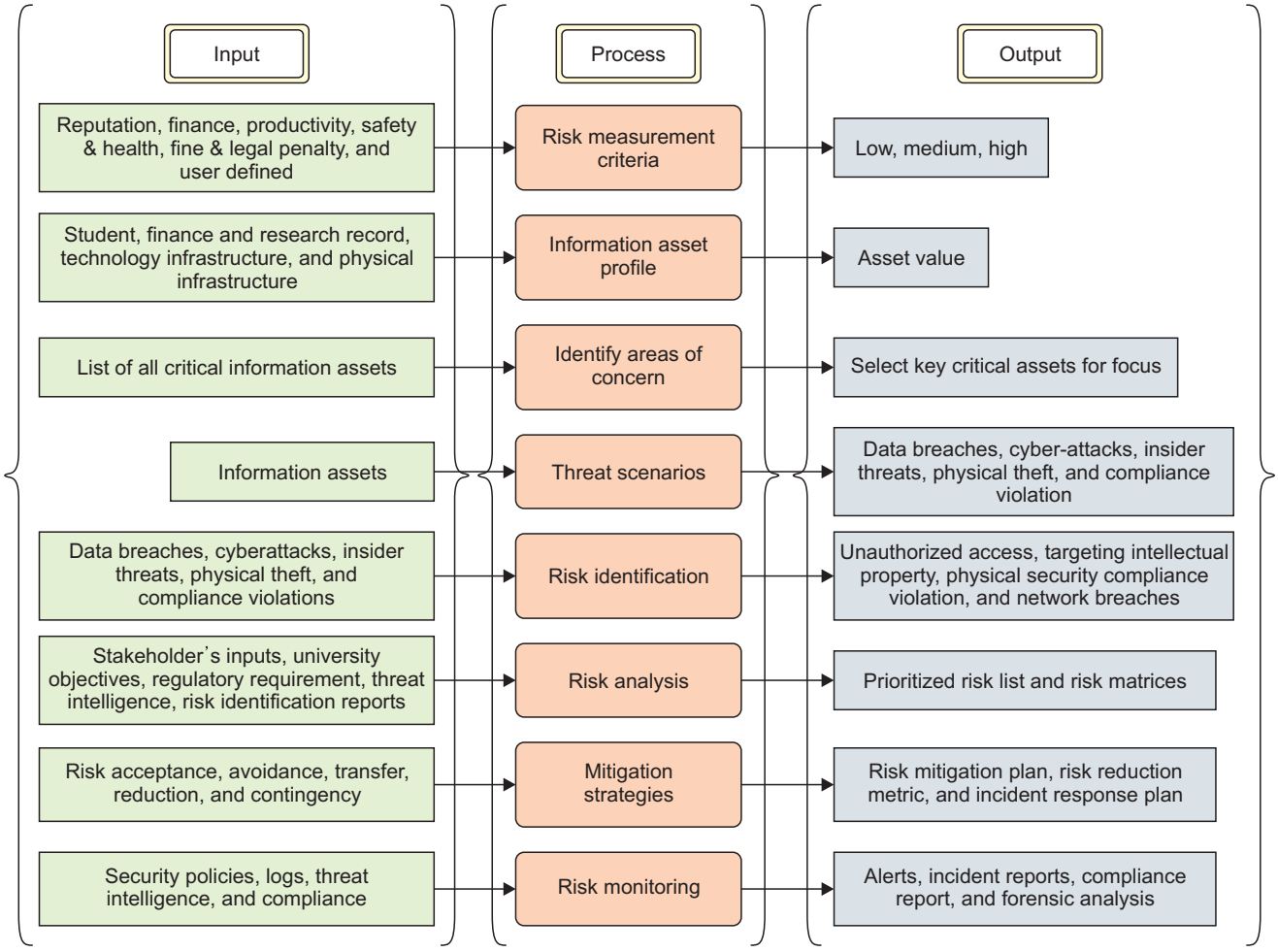


Fig. 4. Framework input, process, and output flow chart.

resources for implementation, which makes them difficult to implement in Ethiopian HEIs with limited resources. The proposed framework uses risk measurement criteria that are specific to the local context and a customized asset profiling method, which considers the distinctive information assets of HEIs, including research data, academic systems, and student records. The framework includes two new elements that are absent or underdeveloped in current frameworks: information asset container identification and areas of concern mapping. The framework provides detailed vulnerability assessments between physical and digital domains, which institutions with basic security infrastructure require. The framework includes practical and cost-effective monitoring mechanisms in its review phase to address the continuous oversight gap present in ISO and NIST models. The framework combines global best practices with local adaptability to achieve scalability for developing-country contexts while remaining operational in low-resource settings. Table 9 (Caralli et al., 2007; ISO, 2022; ITU, 2008; NIST, 2012; 2018) shows a comparative analysis of the proposed 9-step framework vs. international standards/frameworks.

8. A COMPARATIVE ANALYSIS OF THE PROPOSED FRAMEWORK VS. RELATED STUDIES

Table 10 (Ansari & Ali ,2021; Araújo et al., 2025; Baleid & Abdullah, 2026; Dawar & Shivarama, 2017; Kiura & Mango, 2017; Njoroge et al., 2019) shows comparative evidence of information security challenges in HEIs across regions. The research conducted in Kenya, India, and Brazil reveals that the problems encountered in Ethiopian HEIs are part of a larger pattern of problems that are common in developing countries. The studies conducted in Kenyan public and private universities have consistently

 https://doi.org/10.1633/JISTaP.2026.14.2.1

Table 9. Comparative analysis of proposed 9-step framework vs. international standards/frameworks

Proposed 9-step framework (Ethiopian HEIs)	ISO/IEC 27001 (ISO, 2022)	NIST SP 800-30/RMF (NIST, 2012; 2018)	ITU-T X.1055 (ITU, 2008)	OCTAVE Allegro (Caralli et al., 2007)	Novelty/added value
Step 1: Establish risk measurement criteria	Defines the parameters for risk assessment, along with the maximum acceptable risks	Risk assessment requires both risk framing and evaluation factors	The standard provides general guidelines for establishing risk assessment criteria	This approach identifies risk impact areas, yet lacks formal scoring systems	Our approach introduces HEI-specific risk assessment scores for academic contexts
Step 2: Develop an information asset profile	The system needs to create an information asset profile, which includes asset inventory classification	The system categorization method with asset criticality evaluation stands out as a key requirement	The standard recommends asset identification processes, yet it does not provide detailed profiling information	The framework identifies critical assets but fails to include academic information in its analysis	Our approach provides standardized academic asset profiling mechanisms
Step 3: Identify information asset containers	Asset locations are described in general terms in this standard	The system uses defined boundaries to establish risk areas but lacks physical container specifications	The standard provides general information about storing information assets	The framework lacks direct guidance for container mapping procedures	Our approach contains explicit container mapping functionalities for higher education institutions
Step 4: Identify areas of concern	The framework requires organizations to identify their vulnerabilities, yet it lacks a structured method for concern identification	Organizational risk context represents a key aspect of this framework	The standard includes general descriptions of potential vulnerabilities	The approach includes steps to identify specific areas of concern during the process	Our approach adapted OCTAVE for HEIs in Ethiopia through this methodology
Step 5: Identify threat scenarios	Organizations must specify threats as part of their assessments, but without a specific HEI-related context	The approach details threat enumeration procedures. The standard provides general information about threat vectors	The framework includes threat scenarios, but their dynamic nature remains limited	The framework includes threat scenarios, but their dynamic nature remains limited	Our approach provides contextualized threat scenarios specifically designed for HEIs
Step 6: Risk identification	The risk assessment process includes this core element	Risk assessment includes this step as one of its fundamental components	General guidance exists for this step in the framework	The framework employs relative impact evaluation methods to determine risks	Our study uses a combination of quantitative and qualitative approaches for risk evaluation in HEIs
Step 7: Risk analysis	The approach requires both qualitative and quantitative risk analysis methods	Multiple analysis approaches are supported by this standard	The framework contains general guidelines for performing analysis activities	The method uses relative impact evaluation to assess risks	Our study uses both quantitative and qualitative risk evaluation methods for HEIs
Step 8: Selection of mitigation approach	All risk management plans need to contain this requirement	Control selection and prioritization are described within the standard framework	The framework presents a wide range of mitigation strategies	Risk mitigation planning receives encouragement in this approach	Our proposed framework provides custom-made mitigation strategies for organizations with limited resources
Step 9: Risk monitoring and review	The framework demands that organizations develop continuous improvement cycles	The framework requires ongoing continuous monitoring as its core requirement	The framework includes instructions for periodic review	The framework addresses monitoring indirectly, but does not provide a detailed approach	The system presents an implementation for monitoring that accommodates limited resources within HEIs

HEIs, higher education institutions; ISO, International Organization for Standardization; NIST, National Institute of Standards and Technology.

shown that there are weak governance structures, low levels of awareness, and insufficient adoption of structured risk management processes. The findings in Indian HEIs are similar to those of the other two countries, in that libraries and ICT departments point out problems with access control and staff training and propose modifications to ISO 27001 that are relevant to their local context. The Brazilian research confirms these concerns by showing that federal universities are aware of the limitations of generic models and are advocating for HEI-specific frameworks that include continuous review and context-sensitive criteria.

These similarities suggest that the proposed nine-step framework can be applied elsewhere. The framework addresses HEI-specific risks through its inclusion of asset container identification (Step 3) and areas of concern (Step 4), and its focus on resource prioritization and low-cost monitoring (Steps 8 and 9), which are relevant to the budgetary and capacity constraints of institutions in the Global South. In addition to Africa, Asia, and Latin America, the framework provides insights for underfunded universities in developed countries where cybersecurity resources may be deprioritized compared to other institutional objectives. Thus, while based on the Ethiopian case, the framework contributes to an international discussion on building resilient, context-aware ISRM strategies in higher education.

9. STUDY LIMITATIONS

Despite having significant contributions to the information security field in general and HEIs in particular, this study has the following limitations. The study chose four HEIs in Ethiopia using a purposive sampling technique, which may limit the generalizability of the findings. It used descriptive statistics, which exclude inferential statistics, and did not employ different statistical techniques for analyzing and mitigating subjective bias. Additionally, the framework was not put into practice or transformed into a prototype or simulation-based demonstration. The study did not evaluate the ISRM practices of other industries; it solely focused on HEIs. Future research works are expected to fill these gaps.

10. CONCLUSIONS

This study investigated current gaps, best practices, and next directions regarding the management of information security risks in HEIs in Ethiopia from the viewpoints of organizational, people, physical, and technological controls. Based on the identified gaps, the study developed a comprehensive information risk management framework as a viable solution. To illustrate the proposed 9-step framework's unique contributions, the study compared it to other well-known international standards and frame-

Table 10. Comparative evidence of information security challenges in HEIs across regions

Country	Study	Key findings	Relevance to proposed 9-step framework
Kenya	Njoroge et al. (2019)	The implementation of IS practices faces obstacles because of insufficient policy enforcement and insufficient awareness	The framework supports both Step 1 (Risk Criteria) and Step 2 (Asset Profiling) by focusing on governance and awareness
Kenya	Kiura & Mango (2017)	Universities operate on informal procedures because they lack standardized risk-identification protocols	The framework supports both Step 6 (Risk Identification) and Step 7 (Risk Analysis)
India	Dawar & Shivarama (2017)	The current models fail to meet requirements, so the researcher develops a dynamic model that follows ISO 27001 standards	The framework supports both Step 2 (Asset Profiling) and Step 5 (Threat Scenarios)
India	Ansari & Ali (2021)	The implementation of IS practices suffers from inadequate access controls and insufficient staff training	The framework mirrors Step 8 (Mitigation) through its emphasis on training and awareness
Brazil	Araújo et al. (2025)	The current risk frameworks lack specificity for higher education	The framework validates both Step 1 (Local Criteria) and Step 9 (Monitoring and Review)
Cross-region	Baleid & Abdullah (2026)	Higher education institutions worldwide encounter persistent problems because of weak governance structures combined with low staff awareness and insufficient financial support	The proposed 9-step model requires a structured, adaptable framework because of its need

HEIs, higher education institutions; IS, information security; ISO, International Organization for Standardization.

 https://doi.org/10.1633/JISTaP.2026.14.2.1

works as well as comparable studies. The literature-based evidence shows that HEIs around the world confront comparable challenges when it comes to information security threats and risks. These similarities imply that other HEIs could adopt the suggested nine-step structure.

From an organizational control perspective, the absence of an information security policy was considered a key gap, while the familiarity of academic staff with protocols surrounding proper data classification, handling, and access control as well as having a basic understanding of applicable legal, regulatory (such as data protection laws and privacy regulations), or contractual requirements related to information security in their institution is considered as best practices.

From a people control perspective, the absence of an independent reviewer for organization information security policy implementation and operations; lack of awareness, education, and training regarding information security; lack of formalized disciplinary processes when information security policy is violated; and lack of signing non-disclosure agreements in their institution were considered as key gaps, while presence of written responsibilities regarding information security in their job description, awareness of most academic staff about reporting of suspected information security incidents, as well as being knowledgeable about common social engineering attack techniques like phishing emails, were considered as best practices.

From a physical control perspective, despite understanding the significance of physical security measures, such as locking offices, securing sensitive documents, and quickly reporting any suspicious activities or individuals, the majority of academic staff considered the lack of clear policies and procedures for disposing of physical documents in their institutions.

From technological control perspectives, the presence of compromised information security issues in the last few years; lack of designated information security staff and certified information security professionals within ICT directorates; lack of up-to-date and licensed anti-malware software, patch management, BYOD policy, and regular backup systems; lack of motivation among most ICT staff to stay updated on emerging security risks and new technology trends; and lack of established risk measurement criteria for assessing and managing ICT risks, as well as lack of penetration testing, were considered as key gaps; while presence of inventories or registries of important cyber security assets; availability of specific approaches to manage information security risks associated with third-party software applications; presence of approved business continuity plans, application of encryption techniques, enforcement of access control policies in their institutions, and blocking of malicious websites; and availability of professionals to fix hardware or software issues were considered as best practices in Ethiopian HEIs.

Considering the limited research in the area of the selected topic, this study adopted an exploratory research design and leveraged quantitative and qualitative approaches. The research findings may inspire higher education officials, ministries of education, policymakers, and other concerned bodies to look into open issues and enforce the practical implementation of the Unified ISRM Framework.

Future research works are expected to fill the following gaps. The study chose four HEIs in Ethiopia using a purposive sampling technique, which may limit the generalizability of the findings. It used descriptive statistics, which exclude inferential statistics, and did not employ different statistical techniques for analyzing and mitigating subjective bias. Additionally, the framework was not put into practice or transformed into a prototype or simulation-based demonstration. The study did not evaluate the ISRM practices of other industries; it solely focused on HEIs.

CONFLICTS OF INTEREST

No potential conflict of interest relevant to this article was reported.

REFERENCES

Abebe, G. (2022). Perceived importance of information technology governance for Ethiopian higher educational institutions. *International Research Journal of Engineering and Technology (IRJET)*, 9(12), 1237-1244. https://www.irjet.net/archives/V9/i12/IRJET-V9I12207.pdf

Adane, K. (2020). Threats introduced by Bring Your Own Devices (BYOD) adoption in an Ethiopian higher educational institution: Solutions to security and privacy. *IUP Journal of Information Technology*, 16(2), 7-29. https://iupindia.in/ViewArticleDetails.asp?ArticleID=2779

Al-Ahmad, W., & Mohammed, B. (2015). *A code of practice for effective information security risk management using COBIT 5*. Paper presented at 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), Cape Town, South Africa.

Alenezi, A. (2024). Cybersecurity risks and strategies in learn-

ing services of higher education institutions (HEIs) in developing and emerging countries – a critical scoping review. *The Egyptian Journal of Business Studies,* 48(3), 480-506. https://doi.org/10.21608/alat.2024.373548

Alhassan, M. M., & Adjei-Quaye, A. (2017). Information security in an organization. *International Journal of Computer (IJC)*, 24(1), 100-116. https://doi.org/10.53896/ijc.v24i1.820

Ansari, A. J., & Ali, P. M. N. (2021). Security challenges in central university libraries in India. *Library Philosophy and Practice*, 2021(April), 5299. https://digitalcommons.unl.edu/libphilprac/5299

Araújo, J. G. R., Callado, A. L. C., & Bomfim, E. T. (2025). Risk management in Brazilian federal universities: Evaluating the achievement of strategic objectives. *Revista de Educação e Pesquisa em Contabilidade (REPeC) (Journal of Education and Research in Accounting)*, 19, 1-30. https://doi.org/10.17524/repec.v19.e3803

Baleid, H. M., & Abdullah, M. F. (2026). Cybersecurity in higher education: A systematic review of threats, challenges, and mitigation strategies. *Journal of Science and Technology*, 31(1), 20-27. https://doi.org/10.20428/jst.v31i1.3563

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers & Security,* 86, 350-357. https://doi.org/10.1016/j.cose.2019.07.003

Cacciattolo, M. (2015). Ethical considerations in research. In M. Vicars, S. Steinberg, T. McKenna, & Cacciattolo, M. (Eds.). *The praxis of english language teaching and learning (PELT): Beyond the Binaries: Researching Critically in EFL Classrooms* (pp. 61-79). SensePublishers Rotterdam.

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: Complex or simple? Research case examples. *Journal of Research in Nursing,* 25(8), 652-661. https://doi.org/10.1177/1744987120927206

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE allegro: Improving the information security risk assessment process* (SEI Report CMU/SEI-2007-TR-012). Software Engineering Institute. Pittsburgh, PA, USA. https://doi.org/10.1184/R1/6574790.v1

Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies,* 28(2), 1809-1831. https://doi.org/10.1007/s10639-022-11261-8

Daimi, K., & Peoples, C. (2021). Advances in cybersecurity management. Springer Cham.

Dawar, V. A., & Shivarama, J. (2017). *Design and development of dynamic information security management models for sustainable academic libraries*. https://ir.inflibnet.ac.in/handle/1944/2074

Ejerssa, N. (2018). *Assessment of information security maturity level on Ethiopian public universities* (master's thesis). Addis Ababa University, Addis Ababa, Ethiopia.

Ganesen, R., Bakar, A. A., Ramli, R., Rahim, F. A., & Zawawi, M. N. A. (2022). Cybersecurity risk assessment: Modeling factors associated with higher education institutions. *International Journal of Advanced Computer Science and Applications*, 13(8), 355-362. https://doi.org/10.14569/IJACSA.2022.0130843

Grajek, S. (2015). *Top 10 IT issues, 2015: Inflection point*. https://er.educause.edu/articles/2015/1/top-10-it-issues-2015-inflection-point

Grama, J. (2014). *Just in time research: Data breaches in higher education*. https://library.educause.edu/resources/2014/5/just-in-time-research-data-breaches-in-higher-education

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/27001

International Telecommunication Union. (2008). X.1055 : *Risk management and risk profile guidelines for telecommunication organizations*. https://www.itu.int/rec/T-REC-X.1055-200811-I

International Telecommunication Union (ITU). (2020). *Global cybersecurity index*. ITU Publications.

Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in the university network. *Journal of Information Security and Applications*, 35, 128-137. https://doi.org/10.1016/j.jisa.2017.06.006

Keefa, B., Mayoka, G. K., Nkamwesiga, L., & Nyamadi, M. (2024). Information security in higher education institutions: A systematic literature review. *RSEA Journal*, (2024: 16th ORSEA Conference Proceedings), 302-320. https://doi.org/10.56279/orseaj.C2024.18

Kiura, S. M., & Mango, D. M. (2017). Information systems security risk management (ISSRM) model in Kenyan private chartered universities. *European Journal of Computer Science and Information Technology*, 5(2), 1-15. https://eajournals.org/ejcsit/vol-5-issue-2-april-2017/information-systems-security-risk-management-issrm-model-kenyan-private-chartered-universities/

Kombo, F. S., Mwakalinga, P. G., Kumbo, L. I., Edward, L. M., & Bhalalusesa, N. P. (2023). Assessment of higher education information security risk management practices in Tanzania. *East African Journal of Education and Social Sciences*,

4(3), 229-239. https://eajess.ac.tz/index.php/eajess/en/article/view/453?articlesBySimilarityPage=1

Kumar, R. (2015). *Research methodology: A step-by-step guide for beginners* (4th ed.). SAGE.

Nagar, S. (2018). Introduction to OCTAVE. In S. Nagar (Ed.), *Introduction to OCTAVE: For engineers and scientists* (pp. 1-16). Apress.

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments (Special Publication 800-30 Revision 1)*. https://csrc.nist.gov/pubs/sp/800/30/r1/final

National Institute of Standards and Technology. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy (Special Publication 800-37 Revision 2)*. https://csrc.nist.gov/pubs/sp/800/37/r2/final

National Institute of Standards and Technology (NIST). (2024). *The NIST cybersecurity framework 2.0*. https://doi.org/10.6028/NIST.CSWP.29

National Research Council. (2013). *Professionalizing the nation's cybersecurity workforce?: Criteria for decision-making*. The National Academies Press.

Njoroge, P. M., Ogalo, J., & Ratemo, C. M. (2019). A framework for effective information security risk management in Kenyan public universities. *International Journal of Social Sciences and Information Technology*, 4(10), 1-19. https://www.ijssit.com/main/wp-content/uploads/2019/10/Framework-For-Effective-Information-Security-Risk-Management-In-Kenyan-Public-Universities.pdf

Nkambule, M., & Jansen van Vuuren, J. (2024). Integrating enterprise architecture into cybersecurity risk management in higher education. *International Conference on Cyber Warfare and Security*, 19(1), 501-510. https://doi.org/10.34190/iccws.19.1.2189

PCI Security Standards Council. (2008). *Payment card industry security standards*. https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf

Petersen, R. (2013). *EDUCAUSE response to NIST RFI: Developing a framework to improve critical infrastructure cybersecurity*. https://library.educause.edu/resources/2013/4/educause-response-to-nist-rfi-developing-a-framework-to-improve-critical-infrastructure-cybersecurity

Priest, R. G. (1988). Data protection act. *Bulletin of the Royal College of Psychiatrists,* 12(5), 204. https://doi.org/10.1192/s0140078900020162

Putri, N. L., & Wijaya, A. F. (2023). Information technology risk management in educational institutions using ISO 31000 Framework. *Journal of Information Systems and Informatics,* 5(2), 630-649. https://doi.org/10.51519/journalisi.v5i2.468

Readiness and Emergency Management for Schools Technical Assistance Center. (2017). *Cybersecurity considerations for institutions of higher education (Cybersecurity for Higher Ed fact sheet)*. https://files.eric.ed.gov/fulltext/ED593780.pdf

SANS Institute. (2016). *The Center for Internet Security (CIS) Critical security controls v6.0.* https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

Sikman, L., Latinovic, T., Sarajlic, N., & Sikanjic, G. (2023). A model of sustainable information security management system in higher education institutions. *Journal of Physics: Conference Series,* 2540(1), 012003. https://doi.org/10.1088/1742-6596/2540/1/012003

Sulistyowati, I., & Hari Ginardi, R. V. (2018). *Information security risk management with OCTAVE method and ISO/EIC 27001: 2013 (Case study: Airlangga University)*. Paper presented at 4th International Seminar on Science and Technology, Surabaya, Indonesia.

Suroso, J. S., & Fakhrozi, M. A. (2018). Assessment of information system risk management with OCTAVE Allegro at education institution. *Procedia Computer Science,* 135, 202-213. https://doi.org/10.1016/j.procs.2018.08.167

The British Standards Institution. (n.d.). *ISO/IEC 27001 - Information security management system*. https://www.bsigroup.com/en-IN/products-and-services/standards/iso-iec-27001-information-security-management-system/

U.S. Department of Health and Human Services. (2025). *Summary of the HIPAA privacy rule*. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Yilmaz, R., & Yalman, Y. (2016). A comparative analysis of university information systems within the scope of the information security risks. *TEM Journal,* 5(2), 180-191. https://doi.org/10.18421/tem52-10

Yousif Yaseen, K. A. (2022). Importance of cybersecurity in the higher education sector 2022. *Asian Journal of Computer Science and Technology,* 11(2), 20-24. https://doi.org/10.51983/ajcst-2022.11.2.3448