The University Journal: A Doctoral Association of Eastern Africa (DAEA) Publication
Vol 7(2)

ISSN: 2519-0997 (Print)

A Systematic Literature Review of Cybersecurity Risk Assessment and Management Frameworks in Higher Education Institutions

Beatrice Akoth Owino[1*], Collin Oduor, PhD[2] and Gerald Chege, PhD[3]
[1,2,3]United States International University-Africa
P.O. Box 14634 00800, Kenya
*Email: *[1]beatricej2009@gmail.com; [2]coduor@usiu.ac.ke; [3]gchege@usiu.ac.ke*

***Corresponding author**

Cite: Owino, B.A., Oduor, C., & Chege, G. (2025). A Systematic Review of Cybersecurity Risk Assessment and Management Frameworks in Higher Education Institutions. *The University Journal, 7*(2), 1-14.

Abstract

Cybersecurity threats continue to pose significant risks to higher education institutions (HEIs), which increasingly depend on digital infrastructure for academic, administrative, and research activities. However, the effectiveness of cybersecurity risk assessment and management (CSRA&M) frameworks in addressing these threats within university contexts remains unclear. This study presents a systematic literature review to identify, analyze, and synthesize existing CSRA&M models relevant to HEIs. The review followed the PRISMA methodology to ensure transparency and rigor in article selection and analysis. Peer-reviewed journal articles and academic conference papers were sourced from databases including IEEE Xplore, Scopus, and ScienceDirect. Inclusion criteria focused on studies that applied, evaluated, or discussed CSRA&M frameworks in the context of universities or higher education environments. Findings indicate that frameworks such as ISO 27001, ISO/IEC 27005, OCTAVE, and COBIT are frequently referenced. However, many are not fully tailored to universities' socio-technical and governance structures, particularly in developing regions. The review highlights a need for hybrid, context-sensitive approaches that combine technical controls with strategic planning, stakeholder engagement, and regulatory alignment. This study contributes to the cybersecurity literature by providing a consolidated understanding of how existing frameworks address risk in HEIs and identifying key gaps for future research and model development. It offers insights for academic policymakers, IT leaders, and researchers seeking to strengthen cybersecurity resilience in university settings.

Keywords: Cybersecurity, Risk Assessment, Risk Management, Higher Education Institutions, Information Security

Introduction

The rapid digitization of HEIs has created a dynamic, data-driven learning environment that relies heavily on technology for academic, administrative, and research activities. Universities are now more interconnected than ever, from online learning platforms and cloud-based services to digital libraries and financial management systems. However, this growing digital dependency has also introduced various cyber threats. These include data breaches, ransomware attacks, phishing, and other forms of cybercrime that can disrupt services, compromise sensitive data, and severely damage institutional reputations.

Universities are particularly vulnerable because of their unique characteristics: open-access networks, a diverse user base including students, staff, researchers, and third-party collaborators, and a culture that values freedom of information. These attributes make standard cybersecurity solutions difficult to implement effectively. Moreover, as Kure et al. (2022)

highlighted, the cyber threat landscape rapidly evolves, with attacks becoming more sophisticated and targeted. This necessitates robust and adaptive CSRA&M strategies tailored to the complex environments of HEIs.

While various CSRA&M frameworks exist, such as ISO/IEC 27001, ISO 27005, COBIT, OCTAVE Allegro, and NIST SP 800-30, many were designed for corporate or government settings and assume centralized governance and high resource availability. In contrast, many universities face significant barriers, particularly in developing countries, including limited technical capacity, budget constraints, and a lack of formal cybersecurity governance (Badamasi & Utulu, 2021). As a result, cybersecurity risk management in higher education tends to be reactive, fragmented, and under-resourced.

Existing literature reveals key gaps in cybersecurity risk assessment frameworks for HEIs. Despite increasing cyber threats facing HEIs, the literature on CSRA\&M reveals notable gaps that this study seeks to address. Firstly, although various frameworks such as ISO/IEC 27005, NIST SP 800-30, and COBIT have been mentioned, there is limited systematic mapping of the specific CSRA\&M frameworks currently applied within HEIs, particularly across diverse institutional contexts (Aborujilah et al., 2022). Secondly, existing studies often fail to critically assess these frameworks' effectiveness, adaptability, and contextual relevance within university environments. Most frameworks are designed for corporate settings and may not align with the academic culture, decentralized governance, and budgetary constraints typical of HEIs, highlighting the need for evaluation (Alam, 2022). Finally, while challenges and best practices are occasionally documented, the literature lacks an integrated synthesis that captures the common gaps and practical insights necessary to develop a context-aware model suitable for diverse HEI settings. Addressing these gaps, the research contributes to more effective, institution-specific cybersecurity risk management practices in higher education. To address these gaps, the study conducts a systematic literature review to synthesize and critically assess Cybersecurity Risk Assessment and Management Frameworks in Higher Education Institutions research. The following research questions guide the review:

> **RQ1:** What cybersecurity risk assessment and management frameworks are currently applied in higher education institutions?
>
> **RQ1:** How effective, adaptable, and contextually relevant are these frameworks within the operational and cultural settings of universities?
>
> **RQ1:** What gaps, challenges, and best practices can be synthesized from existing literature to inform the development of a context-aware cybersecurity risk assessment and management model for diverse HEI environments?

This study makes several contributions in addressing the research questions: it identifies and maps existing CSRA&M frameworks used in HEIs, providing a comprehensive overview of current practices. It evaluates these frameworks' effectiveness, adaptability, and contextual relevance within diverse university settings, particularly in developing countries with limited empirical data (Aborujilah et al. 2022). Furthermore, it synthesizes key gaps, challenges, and best practices from the literature to inform the development of a context-aware CSRA&M model. This contributes to advancing cybersecurity governance in HEIs by offering a tailored, practical, and inclusive approach that addresses institutional, technical, and human dimensions often overlooked in existing models (Bada et al., 2014).

Literature Review

The CSRA&M has become increasingly vital for HEIs due to their growing reliance on digital infrastructure, cloud platforms, and sensitive academic and personal data management. As HEIs expand their digital operations, they are exposed to many cyber threats such as phishing, ransomware, and data breaches (Owino, 2020). While numerous CSRA&M frameworks such as ISO/IEC 27005, NIST SP 800-30, OCTAVE, and COBIT have been developed to guide organizations in managing cybersecurity risks, these models are often designed with corporate or governmental environments in mind and lack the contextual adaptability necessary for the academic sector. HEIs, characterized by open-access systems, decentralized governance, and diverse user groups, require frameworks that align with their unique operational and cultural dynamics.

In addressing the first objective, identifying and mapping existing CSRA&M frameworks in HEIs, the literature reveals that institutions often adopt hybrid or modified versions of existing models to accommodate their specific needs. For instance, ISO/IEC 27005 is frequently used for its structured approach to risk analysis, yet it often lacks operational mechanisms suitable for academic environments (Alshaikh et al., 2020). Similarly, OCTAVE provides a flexible, asset-based model but may demand more resources than are available to underfunded universities. Despite widespread use, no universally accepted framework is tailored to the higher education context, indicating a significant gap in the availability of fit-for-purpose models.

Several studies have addressed the second objective to evaluate these frameworks' effectiveness, adaptability, and contextual relevance, highlighting critical limitations. The decentralized IT structures common in universities often hinder the full implementation of standardized frameworks (Ramachandran et al., 2017). Moreover, HEIs frequently face resource constraints, inadequate cybersecurity awareness, and weak enforcement of security policies (Bada et al., 2019). These conditions limit the practical application of existing models, particularly in institutions in developing regions. Research by Aborujilah et al. (2022) and Tarek et al. (2021) emphasizes that many HEIs in Africa and similar contexts lack the institutional capacity to adopt or customize frameworks effectively, thus requiring models that are not only adaptable but also scalable to their local realities. Additionally, frameworks often fail to address emerging cybersecurity risks associated with new technologies, such as IoT devices, online learning platforms, and remote access systems Kombo et al., (2023), further questioning their relevance in modern HEI settings.

Concerning the third objective, which is to synthesize gaps, challenges, and best practices to inform a context-aware model, the literature consistently identifies the neglect of human and organizational factors as a major shortcoming in many frameworks. Bada et al. (2014) stress that human behavior, security culture, and institutional leadership significantly influence the effectiveness of cybersecurity efforts but are often underrepresented in risk assessments. Similarly, Shedden et al. (2010) argue that frameworks developed without stakeholder input tend to lack usability and institutional buy-in, thereby limiting their effectiveness. Furthermore, tools for measuring cybersecurity maturity in HEIs are scarce. While models like CMMI and C2M2 exist, they are rarely validated in academic environments, leading to benchmarking and continuous improvement challenges.

Another critical gap in the literature is the lack of empirical research in the global South. Most existing studies are centered in North America, Europe, and parts of Asia, creating a geographic imbalance in understanding cybersecurity risk in HEIs. This limits the generalizability of

findings and fails to capture the unique socio-technical challenges faced by universities in developing countries (Aborujilah et al., 2022). As a result, current frameworks and best practices may be misaligned with the needs of institutions operating under different regulatory, financial, and technological constraints.

In conclusion, the literature indicates that while CSRA&M frameworks are widely applied, they often lack contextual relevance, adaptability, and stakeholder inclusivity when implemented in HEIs. Key gaps include the underrepresentation of human and institutional dimensions, lack of maturity assessment tools, insufficient empirical research in developing regions, and a failure to address emerging cybersecurity threats. This study contributes by systematically reviewing existing frameworks, evaluating their relevance and effectiveness in higher education settings, and synthesizing key lessons to develop a context-aware, stakeholder-driven CSRA&M model suited to the dynamic and diverse needs of HEIs globally.

Methodology

This study employed an SLR approach to identify, evaluate, and synthesize research related to cybersecurity risk assessment and management (CSRA&M) frameworks in higher education institutions (HEIs). The SLR followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure a transparent, rigorous, and replicable review process.

Search Strategy

To capture a comprehensive and multidisciplinary view of the literature, searches were conducted across the following major academic databases: IEEE Xplore, Scopus**,** ScienceDirect**,** SpringerLink**,** ACM Digital Library, and Google Scholar (used for grey literature and additional peer-reviewed content). The search period was unrestricted to allow both foundational and current literature, but prioritized publications from the last 10 years (2013–2023) to ensure relevance. Keywords and Boolean operators were used in combinations to formulate a search string: (**"**cybersecurity**"** OR **"**information security**"**) AND (**"**risk assessment**"** OR **"**risk management**"** OR **"**risk framework**"** OR **"**security framework**"**)

(**"**higher education institutions**"** OR **"**HEIs**"** OR **"**universities**"** OR **"**tertiary education**"**) AND (**"**framework**"** OR **"**model**"** OR **"**standard**"**)

Inclusion and Exclusion Criteria

The inclusion and exclusion criteria were applied during the selection process to filter studies based on relevance and quality. This review included peer-reviewed journal articles, academic conference papers, and reputable conference papers published between 2013 and 2023. Studies were selected if they focused on cybersecurity risk assessment and/or management frameworks, models, or strategies applicable to HEIs. Only English-language publications with full-text accessibility and clear methodological rigor were considered. Preference was given to studies that addressed technical, organizational, or human factors in the context of CSRA&M within academic environments. Table 1 shows the inclusion & exclusion criteria used in the study.

Table 1: Inclusion and Exclusion Criteria

Inclusion Criteria	Exclusion Criteria
Peer-reviewed journal and conference papers	Non-English language publications
Studies focusing on HEIs	Studies not related to education or university contexts.
Articles addressing CSRA&M frameworks or practices	Articles without methodological or practical application
Conceptual, empirical, or review-based papers	Duplicate studies or incomplete articles

Study Selection

From an initial pool of 426 articles, duplicates and irrelevant papers were removed based on title and abstract screening. A total of 85 articles were shortlisted for full-text review. After applying the inclusion and exclusion criteria, 27 papers were selected for final synthesis. The PRISMA flow diagram illustrates the selection process, as indicated in Figure 1 below.

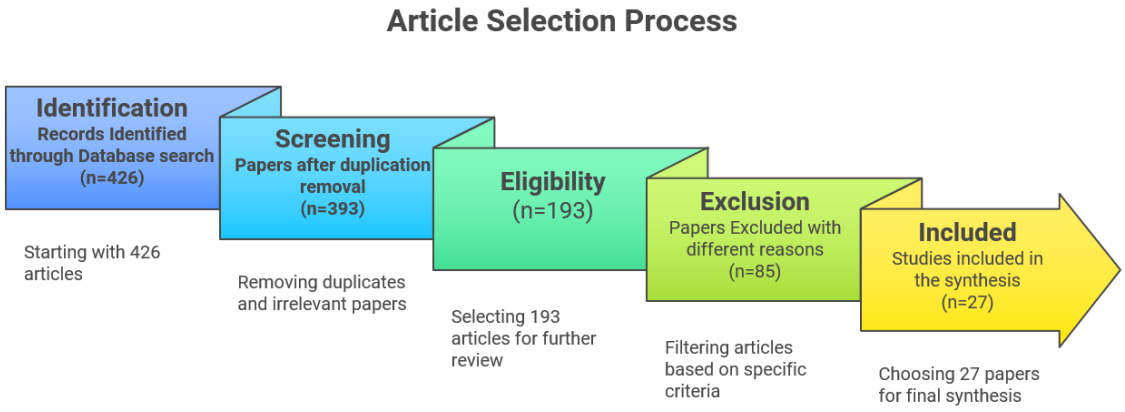

Figure 1: Prisma Diagram

Results

Characteristics of the selected studies

Table 2 summarizes the distribution of the 27 selected articles across major academic databases. Scopus and Google Scholar contributed the highest number of relevant publications (6 each), followed by IEEE Xplore (5), ScienceDirect (4), ACM Digital Library (3), and SpringerLink (3). This distribution highlights the multidisciplinary nature of cybersecurity

research in higher education institutions, with a strong presence across domain-specific and broad academic platforms.

Table 2:Distribution of Reviewed Studies by Database Source

Database	Number of Articles
IEEE Xplore	5
Scopus	6
ScienceDirect	4
SpringerLink	3
ACM Digital Library	3
Google Scholar	6
Total	**27**

Distribution by year

Figure 2 illustrates the yearly distribution of published articles on cybersecurity frameworks in higher education institutions (HEIs) between 2013 and 2023, based on 27 selected studies. The data reveal a gradual increase in scholarly interest over the decade, peaking in 2019 and 2020 with four publications each. This trend indicates growing academic and institutional awareness of cybersecurity challenges in HEIs during this period. A slight decline follows in the last three years (2021–2023), possibly due to shifting research priorities or publication delays. Overall, the chart underscores an upward trajectory in research focus, especially in the latter half of the decade, reflecting the evolving complexity and urgency of cybersecurity issues in higher education settings.

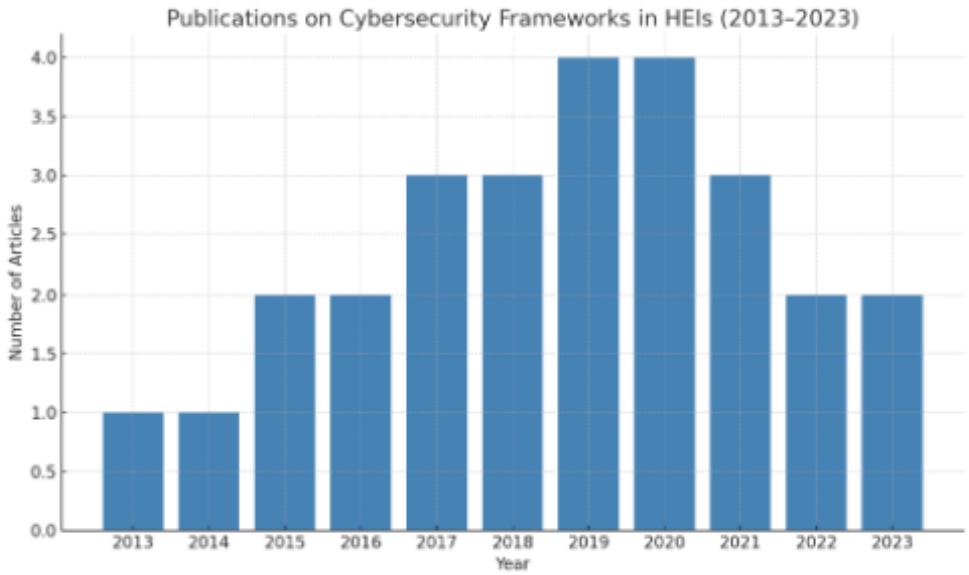

Figure 2: Distribution by year

Results and Synthesis: Based on Research Questions

This systematic literature review aimed to analyze existing CSRA&M frameworks in HEIs, assess their contextual relevance, and synthesize best practices for institutional resilience. Twenty-seven peer-reviewed articles and credible technical studies were reviewed and analyzed according to three key research questions.

RQ1: What cybersecurity risk assessment and management frameworks are applied in higher education institutions?

The review found that ISO 27001 was the most widely referenced framework in the literature, often used as a benchmark for establishing Information Security Management Systems (ISMS) within universities (Makupi & Masese, 2019). ISO/IEC 27005 was also cited as an extension of ISO 27001, offering detailed guidance on risk treatment and evaluation (Dioubate et al., 2022). OCTAVE Allegro emerged as the most contextually adaptive framework, particularly in university environments where stakeholder engagement and qualitative analysis are essential (Sulistyowati & Ginardi; Njoroge).

Other notable frameworks included COBIT and NIST SP 800-30, though these were more prevalent in studies from developed regions with stronger regulatory environments (Aliyu et al.; Haque et al.). Several studies proposed hybrid models combining standards like ISO 27001 and OCTAVE, tailored to specific institutional needs (Aliyu et al., 2020). The summary of the findings is shown in Table 3 below.

Table 3: cybersecurity risk assessment and management frameworks

Framework/Model	Description	Application in HEIs	Source(s)
ISO/IEC 27005	Provides guidelines for information security risk management in support of ISO 27001.	Adopted for structured risk assessment and compliance purposes.	(Salahdine et al., 2021)
NIST SP 800-30	US-based standard offering detailed guidance on risk assessment.	Used in HEIs for identifying, assessing, and mitigating IT-related threats.	Bada et al., (2014); (Almuhammadi & Alsaleh, 2017)
OCTAVE	Organizational risk assessment focusing on operational security risks.	Applied in HEIs for internal risk evaluation and strategic decision-making.	(Dioubate et al., 2022)
FAIR (Factor Analysis of Information Risk)	Quantitative model for measuring and analyzing cybersecurity risk.	Limited adoption in HEIs; used mostly in research or pilot contexts.	(Singh & Joshi, 2017)
COBIT 5/COBIT 2019	Governance and management framework for enterprise IT.	Applied for aligning cybersecurity governance with institutional objectives.	(Binduf et al., 2018); (Tarek et al., 2017)

HEISC Framework	Higher Education Information Security Council's risk management approach.	Specifically developed for U.S. universities to address sector-specific challenges.	(Gichubi et al., 2024)
Custom/Hybrid Models	Institutional adaptations combining multiple standards/frameworks.	Common in developing contexts due to resource or regulatory gaps.	Aborujilah et al. (2022)

The table summarizes cybersecurity risk assessment and management frameworks currently applied in HEIs. It highlights both internationally recognized standards and models tailored for academic environments. ISO/IEC 27005 and NIST SP 800-30 are widely implemented for structured risk management and threat assessment. OCTAVE is used for internal and organizational risk analysis, while FAIR is applied only to quantitative risk modeling. Frameworks like COBIT are used to align IT governance with institutional strategies. The HEISC framework, developed specifically for U.S. universities, addresses sector-specific cybersecurity needs. Many institutions, especially in developing contexts, adopt hybrid or custom models to suit their unique regulatory and resource environments. The table underscores the diversity of frameworks and the adaptive strategies HEIs employ to manage cybersecurity risks effectively.

RQ2: Evaluation of Framework Effectiveness and Contextual Relevance

Most studies highlighted that while ISO-based models provide structured and standardized approaches, they often demand high technical expertise and institutional capacity, making them less accessible to resource-constrained universities (Taherdoost, 2018).In contrast, OCTAVE Allegro offered flexibility through stakeholder-driven assessments and was seen as more applicable in HEIs, particularly in decentralized or less formally governed institutions (Njoroge et al., 2019).

Custom or hybrid models were found to be more effective in adapting to localized challenges, such as those faced by HEIs in developing countries. These frameworks integrate technical standards with institutional characteristics like governance structures, user awareness levels, and risk culture (Dioubate & Daud; Amine et al.). The reviewed literature suggests that a purely technical or one-size-fits-all model is inadequate, particularly given university systems' open-access, heterogeneous nature. Table 4 shows a summary of the findings.

Table 4: Framework Effectiveness and Contextual Relevance

Framework/ Model	Effectiveness in HEIs	Contextual Relevance	Limitations	Source(s)
ISO/IEC 27005	High effectiveness in structured risk identification and mitigation	Moderately relevant; aligns with ISO 27001 in well-resourced institutions.	Resource-intensive; less suitable for small institutions	(Shaikh & Siponen, 2023)
NIST SP 800-30	Strong in technical risk assessment and mitigation	Highly relevant in U.S. HEIs due to federal alignment	Heavy documentation may hinder adoption in	(Bada et al., 2014);

			resource-limited HEIs.	Ramachandran et al. (2017)
OCTAVE	Promotes strategic, organization-wide risk awareness	Well-suited to decentralized academic IT environments.	Limited technical precision and automation.	(Itradat et al., 2014)
FAIR	Enables quantitative risk analysis and cost-benefit insights (Payne, 2017).	Limited practical use in HEIs; mostly piloted in research (Rosenthal et al., 2021).	Requires specialized data and expertise.	(Singh & Joshi, 2017)
COBIT 5/2019	Effective in aligning cybersecurity governance with institutional strategy (Hussain et al., 2022).	Relevant in institutions with mature IT governance (Othman et al., 2018).	Overly complex for small or mid-sized HEIs.	Hussain et al. (2022); Othman et al. (2018)
HEISC Framework	Developed specifically for higher education, supports tailored risk management.	Highly relevant to U.S. HEIs; includes peer benchmarking tools.	Limited adoption outside North America.	(Gichubi et al., 2024)
Custom/Hybrid Models	Varying effectiveness depending on implementation	Highly adaptable to local context in developing countries	Lack of standardization and consistency.	(Aborujilah et al., 2022); Alotaibi & Alfehaid (2021)

RQ3: Synthesis of Gaps, Challenges, and Best Practices

The review identified several gaps in current CSRA&M approaches. First, most frameworks lack explicit consideration of the unique socio-technical environments in HEIs, such as student-led access systems, public networks, and decentralized IT governance (Badamasi & Utulu; Haque et al.). Second, limited research addresses integrating human factors such as user behavior, awareness, and training into risk assessment models. Third, few studies empirically validate these models within university environments, indicating a need for more implementation-focused research.

Best practices identified include the development of hybrid frameworks that combine the rigor of ISO standards with the contextual adaptability of models like OCTAVE. Studies recommend engaging diverse stakeholders (administrators, IT staff, faculty, and students) in the risk assessment process to identify threats and vulnerabilities accurately (Gerl et al.; Dioubate et al.). Additionally, alignment of cybersecurity strategies with institutional policies and national regulations was considered essential for sustainability and compliance (Aliyu et al.; Fouad).

Discussion

Objective 1: Identification and Mapping of CSRA&M Frameworks in HEIs

The first objective of this review was to identify and map cybersecurity risk assessment and management (CSRA&M) frameworks that have been applied in higher education institutions (HEIs). The results indicate that while various models exist, the most commonly implemented frameworks include ISO 27001, ISO/IEC 27005, OCTAVE Allegro, COBIT, and NIST SP 800-30. ISO 27001 and ISO/IEC 27005 were frequently adopted due to their international

recognition and structured methodology for managing information security risks (Makupi & Masese; Dioubate et al.). However, these frameworks often demand high technical expertise, significant financial investment, and institutional commitment, which may limit their implementation in under-resourced universities, particularly in developing countries (Taherdoost, 2018).

OCTAVE Allegro stood out as a more context-aware model, especially suitable for universities because it integrates qualitative approaches and stakeholder participation (Njoroge; Sulistyowati, & Ginardi). COBIT and NIST frameworks were more prevalent in developed regions and often aligned IT governance with risk management goals (Aliyu et al.; Haque et al.). Several studies also introduced hybrid or institution-specific models that blend the robustness of ISO standards with the contextual relevance of OCTAVE or local governance structures (Titi Ciptaningtyas et al.; Al-Serhani et al.).

Objective 2: Evaluation of Framework Effectiveness and Contextual Relevance

The second objective sought to assess the adaptability and effectiveness of CSRA&M frameworks within university environments. The analysis confirmed that structured frameworks like ISO 27001 offer comprehensive controls and audit mechanisms, often failing to align with universities' unique governance and operational dynamics. HEIs typically operate with decentralized systems, a diverse user base, and a culture of academic freedom, making strict compliance-based frameworks harder to enforce.

In contrast, models like OCTAVE Allegro offer the flexibility required in such environments by emphasizing organizational knowledge and stakeholder-driven risk identification (Sulistyowati & Ginardi). These models were especially effective in universities that lack centralized IT governance or where cybersecurity maturity is still developing. Moreover, the literature emphasizes the need for frameworks that are not only technically sound but also culturally and operationally feasible (Gerl et al.; Dioubate & Daud). Custom or hybrid models emerged as particularly beneficial in universities within developing regions, as they can be adapted to local challenges such as limited staff capacity, inadequate training, or fragmented cybersecurity policy frameworks (Fouad, 2021).

Objective 3: Synthesis of Gaps, Challenges, and Best Practices

The final objective was to synthesize the gaps, challenges, and best practices related to CSRA&M implementation in HEIs. Several recurring challenges were identified across the literature. First, most standardized frameworks were not originally designed with universities in mind, leading to issues of scalability and relevance (Badamasi & Utulu, 2021). Second, there is a notable lack of integration of human and behavioral elements in risk assessments, even though many cyber incidents in HEIs stem from user errors, lack of awareness, or poor compliance (Haque et al., 2023).

Best practices highlighted include adopting a hybrid approach that combines elements of ISO 27001 with participatory models like OCTAVE. Engaging diverse stakeholders from IT professionals and administrators to faculty and students was essential to creating accurate and sustainable cybersecurity strategies (Njoroge; Gerl et al.). Additionally, aligning institutional cybersecurity policies with national regulations, such as GDPR or local data protection laws, was vital for compliance and long-term resilience (Aliyu et al., 2020).

Conclusion

This systematic literature review reveals that while multiple cybersecurity risk assessment and management frameworks exist, no single model fully meets the unique needs of higher education institutions. ISO 27001 and similar structured models offer comprehensive technical controls but are often too rigid or resource-intensive for many universities. Conversely, frameworks like OCTAVE Allegro provide flexibility and contextual adaptability but may lack the precision and auditability of formal standards.

The review underscores the need for hybrid, context-sensitive models considering institutional governance, cultural dynamics, and resource availability. Such models should integrate technical and human dimensions of cybersecurity risk and actively involve stakeholders across the institution in the design and implementation process.

In the future, universities should prioritize developing or adapting cybersecurity frameworks that balance global best practices with local realities, especially in resource-limited or developing contexts. Further empirical research and case studies are also recommended to validate and refine these hybrid approaches based on practical outcomes.

References

Aborujilah, A., Al-Othmani, A. Z., Hussien, N. S., Mokhtar, S. A., Long, Z. A., & Nizam, M. (2022). Cybersecurity Risk Assessment Approach for Malaysian Organizations: Malaysian Universities as Case Study. *2022 9th International Conference on Electrical and Electronics Engineering, ICEEE 2022*, 440–450. https://doi.org/10.1109/ICEEE55327.2022.9772546

Alam, M. S. (2022). Need of Cyber Security in Higher Education in Present Era. *International Journal of Creative Research Thoughts*, *10*(3), 2320–2882. www.ijcrt.org

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences (Switzerland)*, *10*(10). https://doi.org/10.3390/app10103660

Almuhammadi, S., & Alsaleh, M. (2017). *I NFORMATION S ECURITY M ATURITY M ODEL F OR NIST C YBER S ECURITY*. 51–62.

Bada, M., Sasse, A., & Bada, M., Sasse, A., Nurse, J. (2014). Cyber Security Awareness Campaigns: Why They Fail to Change Behavior. *International Conference on Cyber Security for Sustainable Society*, *July*, 38.

Badamasi, B., & Utulu, S. C. A. (2021). Framework for Managing Cybercrime Risks in Nigerian. *Proceedings of the 1st Virtual Conference on Implications of Information and Digital Technologies for Development, 2021*, 853–866.

Binduf, A., Alamoudi, H. O., Balahmar, H., Alshamrani, S., Al-Omar, H., & Nagy, N. (2018). Active Directory and Related Aspects of Security. *21st Saudi Computer Society National Computer Conference, NCC 2018*, 4474–4479. https://doi.org/10.1109/NCG.2018.8593188

Dioubate, B. M., Daud, W., & Norhayate, W. (2022). Cyber Security Risk Management Frameworks Implementation in Malaysian Higher Education Institutions. *International Journal of Academic Research in Business and Social Sciences*, *12*(4). https://doi.org/10.6007/ijarbss/v12-i4/12300

Fouad, N. S. (2021). *Securing higher education against cyberthreats : from an institutional risk to a national policy challenge*. https://doi.org/10.1080/23738871.2021.1973526

Gerl, A., von der Heyde, M., Grob, R., Seck, R., & Watkowski, L. (2020). Applying COBIT 2019 to IT Governance in Higher Education. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)*, *P-307*, 517–530. https://doi.org/10.18420/inf2020_47

Gichubi, P. M., Maake, B., & Chweya, R. (2024). Cybersecurity Framework for Kenyan Universities in Conformity with ISO/IEC 27001:2022 Standard. *OALib*, *11*(08), 1–15. https://doi.org/10.4236/oalib.1110810

Haque, M. A., Ahmad, S., John, A., Mishra, K., Mishra, B. K., Kumar, K., & Nazeer, J. (2023). Cybersecurity in Universities: An Evaluation Model. *SN Computer Science*, *4*(5). https://doi.org/10.1007/s42979-023-01984-x

Itradat, A., Sultan, S., Al-Junaidi, M., Qaffaf, R. A., Mashal, F. A., & Daas, F. (2014). Developing an ISO27001 Information Security Management System for an Educat...: חיפוש. *Jordan Journal of Mechanical and Industrial Engineering*, *8*(2), 102. http://eds.b.ebscohost.com.proxy1.athensams.net/eds/detail/detail?sid=ad4bba9d-557d-49d2-8718-6d9c1103c571%40sessionmgr115&crlhashurl=login.aspx%253fdirect%253dtrue%2526profile%253dehost%2526scope%253dsite%2526authtype%253dcrawler%2526jrnl%253d19956665%25

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, *34*(18), 15241–15271. https://doi.org/10.1007/s00521-022-06959-2

Makupi, D., & Masese, N. (2019). *Determining Information Security Maturity Level of an organization based on ISO 27001*. *6*(7), 1–7.

Njoroge, P. M. (2021). An Examination of Threats facing Assets in Use in Kenyan Public Universities. *International Journal of Scientific and Research Publications ·*, *May*. https://doi.org/10.29322/IJSRP.11.05.2021.p11372

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*, *October*.

Owino, B. A. (2020). *AN EMPIRICAL ASSESSMENT OF AUDIT TOOLS FOR*.

Said Kombo, F., Godwin Mwakalinga, P., Inon Kumbo, L., Mihayo Edward, L., & Phillip Bhalalusesa, N. (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://doi.org/10.46606/eajess2023v04i03.0294

Salahdine, F., Mrabet, Z. El, & Kaabouch, N. (2021). Phishing Attacks Detection A Machine Learning-Based Approach. *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 250–255. https://doi.org/10.1109/UEMCON53757.2021.9666627

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers and Security*, *124*, 102974. https://doi.org/10.1016/j.cose.2022.102974

Singh, U. K., & Joshi, C. (2017). Information security risk management framework for University computing environment. *International Journal of Network Security*, *19*(5), 742–751. https://doi.org/10.6633/IJNS.201709.19(5).12

Taherdoost, H. (2018). A review of technology acceptance and adoption models and theories. *Procedia Manufacturing*, *22*(April), 960–967. https://doi.org/10.1016/j.promfg.2018.03.137

Tarek, M., Mohamed, E. K. A., Hussain, M. M., & Basuony, M. A. K. (2017). The implication of information technology on the audit profession in developing country. *International Journal of Accounting & Information Management*, *25*(2), 237–255. https://doi.org/10.1108/ijaim-03-2016-0022

Aborujilah, A., Al-Othmani, A. Z., Hussien, N. S., Mokhtar, S. A., Long, Z. A., & Nizam, M. (2022). Cybersecurity Risk Assessment Approach for Malaysian Organizations: Malaysian Universities as Case Study. *2022 9th International Conference on Electrical and Electronics Engineering, ICEEE 2022*, 440–450. https://doi.org/10.1109/ICEEE55327.2022.9772546

Alam, M. S. (2022). Need of Cyber Security in Higher Education in Present Era. *International Journal of Creative Research Thoughts*, *10*(3), 2320–2882. www.ijcrt.org

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences (Switzerland)*, *10*(10). https://doi.org/10.3390/app10103660

Almuhammadi, S., & Alsaleh, M. (2017). *I NFORMATION S ECURITY M ATURITY M ODEL F OR NIST C YBER S ECURITY*. 51–62.

Bada, M., Sasse, A., & Bada, M., Sasse, A., Nurse, J. (2014). Cyber Security Awareness Campaigns: Why They Fail to Change Behavior. *International Conference on Cyber Security for Sustainable Society*, *July*, 38.

Badamasi, B., & Utulu, S. C. A. (2021). Framework for Managing Cybercrime Risks in Nigerian. *Proceedings of the 1st Virtual Conference on Implications of Information and Digital Technologies for Development, 2021*, 853–866.

Binduf, A., Alamoudi, H. O., Balahmar, H., Alshamrani, S., Al-Omar, H., & Nagy, N. (2018). Active Directory and Related Aspects of Security. *21st Saudi Computer Society National Computer Conference, NCC 2018*, 4474–4479. https://doi.org/10.1109/NCG.2018.8593188

Dioubate, B. M., Daud, W., & Norhayate, W. (2022). Cyber Security Risk Management Frameworks Implementation in Malaysian Higher Education Institutions. *International Journal of Academic Research in Business and Social Sciences*, *12*(4). https://doi.org/10.6007/ijarbss/v12-i4/12300

Fouad, N. S. (2021). *Securing higher education against cyberthreats : from an institutional risk to a national policy challenge*. https://doi.org/10.1080/23738871.2021.1973526

Gerl, A., von der Heyde, M., Grob, R., Seck, R., & Watkowski, L. (2020). Applying COBIT 2019 to IT Governance in Higher Education. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)*, *P-307*, 517–530. https://doi.org/10.18420/inf2020_47

Gichubi, P. M., Maake, B., & Chweya, R. (2024). Cybersecurity Framework for Kenyan Universities in Conformity with ISO/IEC 27001:2022 Standard. *OALib*, *11*(08), 1–15. https://doi.org/10.4236/oalib.1110810

Haque, M. A., Ahmad, S., John, A., Mishra, K., Mishra, B. K., Kumar, K., & Nazeer, J. (2023). Cybersecurity in Universities: An Evaluation Model. *SN Computer Science*, *4*(5). https://doi.org/10.1007/s42979-023-01984-x

Itradat, A., Sultan, S., Al-Junaidi, M., Qaffaf, R. A., Mashal, F. A., & Daas, F. (2014). Developing an

ISO27001 Information Security Management System for an Educat...: חיפוש. *Jordan Journal of Mechanical and Industrial Engineering*, *8*(2), 102. http://eds.b.ebscohost.com.proxy1.athensams.net/eds/detail/detail?sid=ad4bba9d-557d-49d2-8718-6d9c1103c571%40sessionmgr115&crlhashurl=login.aspx%253fdirect%253dtrue%2526profile%253dehost%2526scope%253dsite%2526authtype%253dcrawler%2526jrnl%253d19956665%25

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, *34*(18), 15241–15271. https://doi.org/10.1007/s00521-022-06959-2

Makupi, D., & Masese, N. (2019). *Determining Information Security Maturity Level of an organization based on ISO 27001*. *6*(7), 1–7.

Njoroge, P. M. (2021). An Examination of Threats facing Assets in Use in Kenyan Public Universities. *International Journal of Scientific and Research Publications ·*, *May*. https://doi.org/10.29322/IJSRP.11.05.2021.p11372

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*, *October*.

Owino, B. A. (2020). *AN EMPIRICAL ASSESSMENT OF AUDIT TOOLS FOR*.

Said Kombo, F., Godwin Mwakalinga, P., Inon Kumbo, L., Mihayo Edward, L., & Phillip Bhalalusesa, N. (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://doi.org/10.46606/eajess2023v04i03.0294

Salahdine, F., Mrabet, Z. El, & Kaabouch, N. (2021). Phishing Attacks Detection A Machine Learning-Based Approach. *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 250–255. https://doi.org/10.1109/UEMCON53757.2021.9666627

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers and Security*, *124*, 102974. https://doi.org/10.1016/j.cose.2022.102974

Singh, U. K., & Joshi, C. (2017). Information security risk management framework for University computing environment. *International Journal of Network Security*, *19*(5), 742–751. https://doi.org/10.6633/IJNS.201709.19(5).12

Taherdoost, H. (2018). A review of technology acceptance and adoption models and theories. *Procedia Manufacturing*, *22*(April), 960–967. https://doi.org/10.1016/j.promfg.2018.03.137

Tarek, M., Mohamed, E. K. A., Hussain, M. M., & Basuony, M. A. K. (2017). The implication of information technology on the audit profession in developing country. *International Journal of Accounting & Information Management*, *25*(2), 237–255. https://doi.org/10.1108/ijaim-03-2016-0022