International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

SYSTEMATIC REVIEW OF CYBERSECURITY FRAMEWORKS FOR HIGHER EDUCATION INSTITUTIONS: CHARACTERISTICS, COMPONENTS, AND CHALLENGES

Milagros B. Barruga

University of the Cordilleras, Baguio City, Philippines

mbbarruga@mmsu.edu.ph

Abstract

Higher Education Institutions (HEIs) are becoming more vulnerable to cybersecurity threats due to their open and diverse systems and reliance on digital infrastructure for academic and administrative operations. This systematic literature review (SLR) investigates the characteristics, components, and challenges of cybersecurity frameworks tailored to HEIs. The study aims to consolidate insights from global and localized research to serve as a basis for developing effective and context-aware cybersecurity strategies. The review synthesizes 50 peer-reviewed studies published between 2010 and 2024. The results reveal that effective cybersecurity frameworks for HEIs must exhibit comprehensiveness (66% of mentions) and adaptability (grouped characteristics around 50%) to accommodate academic environments' dynamic and decentralized nature. Key components identified include awareness and training (52%), policy compliance mechanisms (52%), and continuous improvement practices (48%), which are critical for protecting institutional assets. Common implementation challenges include resource constraints (88%), implementation complexity (62%), cultural resistance (58%), and the evolving threat landscape (58%). These results demonstrate the discrepancy between existing frameworks and the actual operational reality of HEIs. This review contributes to the field by offering a structured synthesis of what constitutes a practical cybersecurity framework for HEIs grounded in empirical and conceptual research. It also establishes a foundation for further studies exploring the contextual adaptation of cybersecurity standards in academic settings

Index Terms— cybersecurity, frameworks, characteristics, components, challenges, higher education institution

I. INTRODUCTION

As reliance on information technology grows, cyberattacks become more attractive and destructive [1]. In the modern digital landscape, the significance of cybersecurity cannot be overstated. It encompasses protecting sensitive data [2], [3], national security [6] [3], and organizational reputation [1] [6] while ensuring compliance with regulations [7], [8] [10], financial sustainability [6], [7], and resilience [11] [3].

Knowledge creation, storage, and dissemination depend heavily on HEIs. However, HEIs are now more vulnerable to cybersecurity threats due to their rising reliance on digital administration, research, and education platforms. Cybercriminals are drawn to universities

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and colleges because they hold sensitive data, including private student records and confidential research data [12] [13]. They are excellent targets for cybercriminals looking to take advantage of the sensitive research data and vast amounts of personal information they store [14], [15]. Strong cybersecurity measures are necessary to avoid data breaches and illegal access, as the integrity of current research is crucial for preserving academic reputation and confidence [16].

HEIs face a significant increase in cyber threats due to their collaborative, open, and decentralized environment, where the balance between security and academic freedom poses unique challenges. HEIs have a culture emphasizing openness and the free exchange of ideas [17] [18]. This environment can lead to vulnerabilities, as it intentionally lowers barriers to access [14], [15]. Many HEIs operate with decentralized IT structures, which create multiple entry points for cyber threats [15]. Different departments manage their resources. This can lead to inconsistent security measures and a lack of coordination in response to threats [14], [15], challenging comprehensive security. While other industries also handle sensitive data, the nature and volume of academic research data can require stricter standards for integrity and confidentiality [19]. In contrast, many businesses operate under more stringent access controls to safeguard sensitive information, which could benefit from a more closed-off approach than academia. Industries with centralized IT infrastructures often have standardized security protocols that simplify monitoring and management [20].

In addition to these vulnerabilities, HEIs must comply with legal and regulatory requirements on data protection, privacy laws, and research integrity standards, which call for strong cybersecurity procedures [14], [15]. HEIs typically handle a wider range of compliance concerns in several operational domains, which affects their cybersecurity strategies. The rapid increase in cyberattacks requires HEIs to develop effective incident response strategies to mitigate damages and recover from breaches swiftly [12], [15]. Moreover, increasing cybersecurity awareness and educating stakeholders is essential for lowering susceptibility to phishing and other threats, especially in light of academia's open atmosphere [14]. HEIs deal with constant staff, faculty, and student turnover. Attack vulnerability may increase if new users are not adequately trained in cybersecurity protocols [15]. HEIs frequently oversee vital infrastructure for the organization and the community at large. Hence, specialized cybersecurity measures are required to guarantee ongoing operational availability [14], [15], [20]. The COVID-19 pandemic forced a transition to online education, heightened cyberthreats, necessitating HEIs to safeguard remote access and shield their networks from more external connections [15], [21]. Personal devices connecting to university networks create many possible entry points for hackers as remote teaching and learning become more popular [22]. Strict regulations are required because the widespread use of personal devices (BYOD) in classrooms raises the possibility of institutional networks being vulnerable to cybersecurity attacks [1], [14]. The fast-paced adoption of emerging and innovative technologies (such as cloud computing, e-learning platforms, and IoT devices) outpaces the ability to secure systems effectively [23]. Due to financial limitations, many HEIs cannot invest in cybersecurity solutions, infrastructure, and knowledgeable staff [15]. Corporations often have larger budgets for cybersecurity, allowing for more advanced technologies and professional staff [24]. The diverse range of stakeholders and fragmented leadership in HEIs can make developing a uniform cybersecurity policy [14] more challenging. Generally speaking, commercial

Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

enterprises have simpler hierarchical structures that can speed up policy enforcement and decision-making [25].

An organized method for managing and lowering cybersecurity risks, a cybersecurity framework gives businesses rules, norms, and principles. Frameworks can cover various topics, such as technology, procedures, and governance, that are frequently created using best practices [26], [27]. Organizations can create strong security measures against cyberattacks using general tools and techniques in cybersecurity frameworks. Notable cybersecurity frameworks include the NIST Cybersecurity Framework [9], [28], ISO/IEC 27001 [27], [29], [30], and CIS Controls [9], [11]. These frameworks share foundational requirements that ensure consistency, compliance, and resilience across sectors [27]. Some cross-industry cybersecurity framework requirements include risk assessment [6], [9], compliance with regulations [26], [27], incident response planning [11], employee training and awareness [5], [31], data protection and privacy [26], [27], continuous monitoring and improvement [11], [32], [33], and interoperability [1], [27].

While cybersecurity frameworks exist for various industries, those specifically designed for HEIs often exhibit specific gaps compared to more generalized or cross-industry frameworks. Despite the abundance of general cyber threat literature, there is a lack of targeted research on cybersecurity threats in higher education [13]. These strategies may not fully address the distinctive operational, cultural, and technological landscape of the HEIs [34].

HEIs require continuous assessment and improvement of their cybersecurity frameworks to identify and address weaknesses effectively in a constantly evolving threat landscape [14], [15], [24]. However, HEIs contend with unique threats that are not explicitly discussed in broader frameworks. Issues such as academia's open and collaborative nature can render specific cross-industry strategies ineffective against vulnerabilities inherent in educational environments [14]. The risk of data breaches involving student personal information and sensitive intellectual property can be significantly higher in universities than in industries focused on profit [19]. Many business organizations operate under centralized IT controls, whereas HEIs often lack cohesive governance, leading to fragmented security postures that cross-industry frameworks may not account for [14], [15]. Moreover, cross-industry frameworks may not tailor their compliance guidance to account for the nuances of educational regulations and the handling of student data [20], [24], [26].

For-profit organizations can often allocate dedicated cybersecurity teams and considerable financial resources. In contrast, budgetary and staffing constraints impact many HEIs' security implementations. Many broad frameworks lack tailored training and awareness initiatives pertinent to HEIs. The effectiveness of security protocols relies heavily on user awareness and training, which needs to be contextualized for the academic environment. While HEIs must create instructive and captivating programs catered to staff and students' unique requirements and behaviors, cross-industry frameworks may offer generalized training ideas. Cross-industry frameworks may not adequately address the rapid adoption and integration of new academic technologies by HEIs, such as learning management systems and mobile applications. Frameworks like ISO 27001 may lack guidance on managing specific risks posed by emerging educational technologies frequently utilized in HEIs [4]. The academic focus on openness can lead to resistance against policies that are perceived as limiting collaboration or access to information, unlike the corporate environments where compliance is more strictly enforced [7],

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[21], [31]. Cross-industry frameworks typically outline standardized response procedures that may not operationally fit the diverse needs of academia, where research continuity or class schedules might be directly impacted [11], [14], [26].

Specific strategies must be used to handle the particular difficulties educational institutions face [13]. The effectiveness of cybersecurity procedures in the education sector can be significantly increased by taking a more nuanced approach that considers the decentralized nature of IT, conforms with sector rules, and considers institutional culture [14].

A systematic literature review (SLR) determines which essential cybersecurity elements should be included in a cybersecurity framework designed explicitly for HEIs. This study seeks to close the research gap by examining current cybersecurity frameworks and identifying their key traits, elements, and difficulties pertinent to the HEI environment. By methodically evaluating the body of existing research, the main goal of this study is to investigate the crucial cybersecurity considerations for HEIs. This SLR specifically fills the following research gaps: a) the characteristics of an effective cybersecurity framework for HEIs; b) the key components of cybersecurity frameworks designed for HEIs; and c) the challenges in implementing cybersecurity frameworks in HEIs. The study will lay the groundwork for improving cybersecurity strategies that meet the particular operational and security needs of HEIs by answering these concerns.

This paper employs a systematic literature review process to uncover pertinent papers, extract critical data, and synthesize ideas into creating cybersecurity frameworks focusing on HEIs. With multiple frameworks proposed or adopted in various situations and geographies, the literature on cybersecurity frameworks in HEIs is vast but dispersed. Few studies have examined how these frameworks fit with the distinctive features of HEIs. The gaps in present approaches are highlighted, and critical areas that require further attention are identified as this study examines the literature on cybersecurity frameworks, key components, characteristics, and challenges unique to HEIs.

II. METHOD

This study uses a systematic literature review (SLR) technique to find, evaluate, and compile pertinent research on cybersecurity frameworks for HEIs. This method guarantees a thorough and repeatable procedure for addressing the research questions by adhering to Kitchenham's recommendations for conducting systematic software engineering reviews. The research questions are as follows:

RQ1: What are the defining characteristics of cybersecurity frameworks in HEIs?

RQ2: What are the key components of cybersecurity frameworks in HEIs?

RQ3: What are the implementation challenges of cybersecurity frameworks in HEIs?

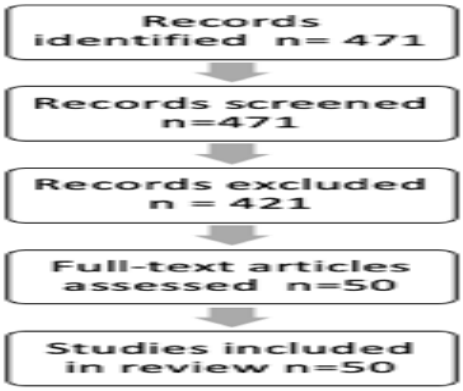
For this review, opportunistic searches in Scopus, ACM Digital Library, IEEE Xplore, and ScienceDirect were used in addition to Google Scholar. A structured search string was created to find research on cybersecurity frameworks designed explicitly for HEIs, their features, essential elements, and the difficulties in implementing them. The following is the Google Scholar search string:

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

"cybersecurity framework" OR "information security framework" OR "security framework" AND ("higher education" OR university OR college OR "academic institution")
AND (characteristics OR components OR challenges OR adoption OR implementation OR evaluation)
-exclude "enterprise" -exclude "corporate" -exclude "business"
After:2014
The scope of this investigation required restricting the dataset to the top 50 papers scored by relevance, even though Google Scholar initially produced almost 18,000 hits. Manual screening was used to weed out articles that did not align with the research goals, such as those that focused on corporate or irrelevant institutional frameworks (see Figure 1).

Figure 1. PRISMA-style flow diagram showing the selection process



The inclusion criteria were limited to peer-reviewed journal articles and conference proceedings published between 2014 and 2024, written or translated in English, and addressing cybersecurity frameworks applicable to HEIs. However, one study from 2010 was deliberately included due to its strong thematic relevance to the research objectives, particularly in the context of framework development for academic institutions. Articles explicitly proposing, evaluating, or discussing cybersecurity frameworks for HEIs, written or translated in English, and those addressing at least one of the three research questions—characteristics, components, or challenges of cybersecurity frameworks—were extracted. On the other hand, articles focused on corporate cybersecurity frameworks or other unrelated sectors and studies without empirical evidence were excluded.
A standardized data extraction form was employed to collect essential information from each article, including bibliographic details (title, authors, year, and source), study methodology, framework discussed or introduced, and findings related to the characteristics, components, and challenges of cybersecurity frameworks for HEIs. The extracted data were synthesized into themes aligned with the research questions, enabling a structured and comprehensive literature analysis.
A weighted scoring system based on methodological rigor, empirical evidence, and relevance to the research questions was applied to ensure the rigor of the included studies. Only articles meeting a threshold quality score were included in the final synthesis.

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

III. RESULTS AND DISCUSSION

This comprehensive literature evaluation considered 50 peer-reviewed studies from 2010 to 2024. With a noticeable increase in publications starting in 2020, the distribution of research shows a growing scholarly interest in the cybersecurity posture of HEIs. Reputable conferences and journals, such as IEEE, Computers and Security, Applied Sciences, and PeerJ, provided the reviewed studies.

Based on the type of inquiry and methodology, the studies were divided into seven main research typologies. Literature reviews accounted for the most significant percentage (26%), closely followed by Empirical qualitative studies (26%). Applied and implementation-based research comprised 10% of the papers, while Conceptual or theoretical models comprised 14%. The distribution of the remaining typologies among Mixed-Methods Research, Comparative/Evaluative Studies, and Quantitative Approaches reflected a fair diversity of methodological viewpoints. This grouping shows HEIs have a solid basic understanding of cybersecurity backed by applied research and conceptual development.

Geographically, the reviewed studies originated from multiple continents, indicating a global recognition of cybersecurity needs in academic settings. Asia contributed the largest share (32%), with active research coming from countries such as Malaysia, Indonesia, Saudi Arabia, and the Philippines. Europe followed (16%), including works from the UK, Norway, and the Netherlands. North America (12%), Africa (8%), and South/Central America (4%) were also represented, while approximately 14% of studies adopted a global or cross-contextual scope. This spread reflects a geographically inclusive perspective and emphasizes the universality of cybersecurity challenges in higher education.

Regarding framework orientation, 62% of the studies proposed or evaluated novel models, tools, or strategies designed explicitly for HEIs, including frameworks like HCYMAF, SCMAF, and the Cybersecurity Conceptual Framework. The remaining 38% examined or adapted existing frameworks such as NIST, ISO/IEC 27001, and other best-practice models, offering comparative insights or context-based applications [30]. These results indicate a healthy balance between innovation and adherence to established cybersecurity standards.

Table 1 presents a condensed synthesis of selected cybersecurity frameworks, models, and tools ident through the systematic literature review. While 50 peer-reviewed studies were analyzed, this representative subset exemplifies the diversity of approaches and thematic relevance across the three principal research questions.

Table I. Synthesis of Framework Characteristics, Components, and Challenges Addressing HEIs' Cybersecurity

Index	Framework/Model /Tool/Strategy	RQ1 themes (Characteristics)	RQ2 themes (Key components)	RQ3 themes (Challenges)
1	Blockchain-based cybersecurity framework [35]	Decentralized, Immutable, Transparent, Secure, Automated,	Blockchain system infrastructure and interfaces, Access control	Implementation complexity, Cultural resistance,

Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Index	Framework/Model /Tool/Strategy	RQ1 themes (Characteristics)	RQ2 themes (Key components)	RQ3 themes (Challenges)
		Consensus-based, Scalable, User-controlled, Auditable, Interoperable		Regulatory compliance, Scalability issues, Cost of integration, Need for training and awareness
4	Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) [36]	Integrated, Self-assessing, Maturity-based, Gap-analyzing, Metrics-driven, Adaptable, Continuous-improvement-focused, Validated	Security management, Risk assessment, Incident response, Security awareness and training, Access control, Data protection, Compliance with regulations, Asset management, Technical controls, Continuous monitoring	Complexity of integration, Validation of maturity levels, Inconsistent metrics, User engagement and training, Evolving threat landscape, Measurement of effectiveness
5	Security Maturity Assessment Framework (SCMAF) [34]	Comprehensiveness, Adaptable, Maturity-based, Standards-aligned, User-friendly,	Security requirements, Assessment tools, Risk management, Governance and policy, Continuous improvement	Complexity, Resource constraints, Lack of customization, Integration difficulties, Resistance to change, Measurement of effectiveness
6	Access management ontology [23]	Interoperable, Secure, Semantic, Standardized, User-friendly, Flexible, Comprehensive, Validated	Formal semantic definitions, Access control mechanisms, User interface design, Integration with	Fragmented semantics, Complexity of integration, Evolving threat landscape,

Received: August 08, 2025

Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Index	Framework/Model /Tool/Strategy	RQ1 themes (Characteristics)	RQ2 themes (Key components)	RQ3 themes (Challenges)
			digital twins, Building Information Model (BIM) integration, IoT device interoperability, Competency questions, Policy frameworks, Resource Management	Stakeholder engagement, Resource limitations
9	Cybersecurity Framework Browser (CRUMBS) [37]	Comprehensive, Adaptable, Usable	Contextualization, Visualization	Complexity, Perceived difficulty, Scattered information, Automation requirement, Visual analysis limitations
10	SmartPLS (Partial Least Squares Structural Equation Modeling) [38]	Comprehensive, Integrative, Adaptable	Technical infrastructure, User awareness and training, Incident response protocols, Research utilization, Evaluation metrics	Diverse user groups, Limited resources, Rapidly evolving threat landscape, Resistance to policy changes, Balancing access and security
11	Cybersecurity Conceptual Framework (CSCF) [39]	Comprehensive, Adaptable, International standards-aligned, Best practices-aligned	Tools and technologies, Policies and guidelines, Risk management approaches, Training and awareness programs,	Decentralized networks, Insufficient knowledge of risks, Resistance to change, Resource limitations, Compliance with

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Index	Framework/Model /Tool/Strategy	RQ1 themes (Characteristics)	RQ2 themes (Key components)	RQ3 themes (Challenges)
			Evaluation and assurance mechanisms	diverse standards, Lack of standardization
13	OCTAVE Allegro framework [40]	Structured, Critical assets-focused, Inclusive, Customizable	Asset Identification, Risk assessment, Profile building, Mitigation strategies, Ongoing review	Resource constraints, Awareness and training, Evolving threat landscape, Resistance to change, Inter-departmental coordination
14	Three-stage cybersecurity management framework [41]	Holistic, Strategic, Comprehensive	Risk assessment, Vulnerability identification and mitigation strategies, Training and awareness programs, Incident detection and response protocols, Communication, Containment and eradication, Recovery plans and processes, Incident analysis and lessons learned, Continuous improvement measures for future preparedness	Lack of resources, Resistance to change, Limited cybersecurity expertise, Complexity of implementation, Rapidly evolving threat landscape, Communication challenges

Received: August 08, 2025

Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Each entry in the table summarizes the nature of cybersecurity framework implementations and outlines the corresponding thematic contributions to the study's analytical dimensions: RQ1 (defining characteristics), RQ2 (key components), and RQ3 (implementation challenges). For instance, the blockchain-based cybersecurity framework is characterized by decentralization, immutability, automation, and user control, with technical components focused on access control systems. However, its application is challenged by implementation complexity, scalability issues, regulatory ambiguity, and the need for stakeholder training. Similarly, maturity-oriented frameworks such as HCYMAF and SCMAF underscore adaptability, metrics-driven evaluation, and alignment with standards while addressing institutional components like risk management, continuous monitoring, and training. These models also highlight challenges, including integration difficulties, inconsistent metrics, and resistance to change. The full synthesis matrix, containing detailed extractions from all reviewed studies, is available in the study appendix.

A. Characteristics of Effective Cybersecurity Frameworks for HEIs

The analysis of 50 reviewed studies identified various characteristics essential for effective cybersecurity frameworks tailored to HEIs. These characteristics were thematically clustered into six groups for more precise interpretation. Themes are grouped according to conceptual similarities reflecting strategic focus, user design, governance alignment, and implementation features.

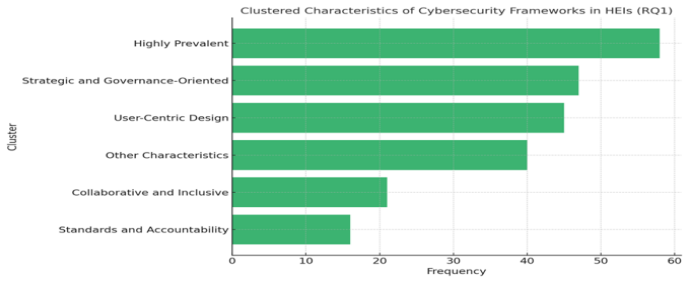
The Highly Prevalent cluster included comprehensiveness and adaptability, which appeared in 33 and 25 studies, respectively, indicating their foundational role in ensuring holistic and responsive frameworks. The Strategic and Governance-Oriented cluster covered characteristics like integration, standard alignment, and policy-driven strategies, totaling 47 mentions, emphasizing the importance of aligning frameworks with institutional structures and strategic objectives. The Collaborative and Inclusive cluster, cited in 21 studies, highlighted stakeholder involvement and organizational inclusivity. Similarly, themes around Standards and Accountability, such as measurability, auditing, and gap analysis, appeared in 16 studies, reflecting a demand for transparent and structured evaluation mechanisms.

The largest thematic group, User-Centric Design, encompassing traits such as flexibility, usability, sustainability, and continuous improvement, was reflected in 47 combined mentions, underscoring the need for human-centric, adaptable systems. Lastly, the Other Characteristics cluster captured less frequently mentioned yet noteworthy features such as multi-layered security, decentralization, and transparency. This clustering approach provides a refined understanding of the core features to consider in designing robust and sustainable cybersecurity frameworks for HEIs. Figure 2 presents the distribution of cybersecurity framework characteristics identified in the reviewed studies.

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 2. Characteristics of Cybersecurity Frameworks in Higher Education Institutions



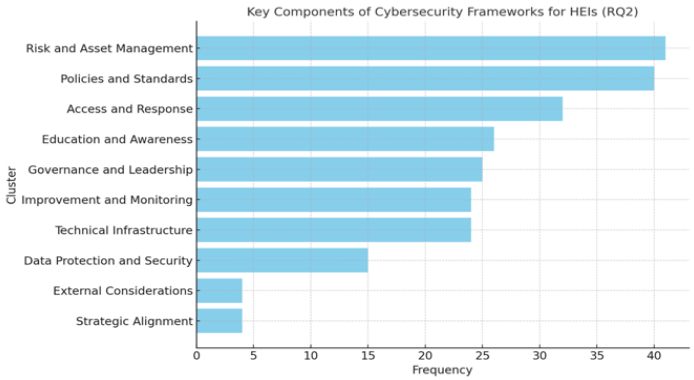
B. Key Components of Cybersecurity Frameworks for Higher Education Institutions

The literature's thematic analysis revealed 17 core components of cybersecurity frameworks for HEIs, which were then organized into 10 thematic clusters. These clusters reflect technical and organizational elements essential for a robust cybersecurity posture. Each component is represented by its frequency of occurrence across the literature and its relative importance in supporting a comprehensive and resilient cybersecurity architecture.

The Education and Awareness and Policies and Standards clusters were the most prominent, each cited in 26 studies, indicating the need for user training and clear, standardized guidelines. Improvement and Monitoring, which include continuous evaluation and feedback mechanisms, were noted in 24 studies, reinforcing the value of ongoing refinement. Components related to Risk and Asset Management (41 mentions) and Technical Infrastructure (24 mentions) underscore the importance of systematic risk identification and the deployment of reliable, secure technologies. Governance-focused components, grouped under Governance and Leadership, appeared in 25 studies, highlighting institutional support and operational procedures as critical enablers.

Other notable clusters included Access and Response (32 mentions), which addressed control mechanisms and incident handling, and Data Protection and Security (15 mentions), which ensured data integrity and confidentiality. Furthermore, although Strategic Alignment and External Considerations appeared less frequently, their presence points to the growing importance of aligning cybersecurity with institutional goals and external threats; these findings collectively highlight a multidimensional framework that balances policy, people, and technology. Figure 3 presents the distribution of key components of the cybersecurity framework identified in the reviewed studies.

Figure 3. Key Components of Cybersecurity Frameworks for Higher Education Institutions



International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

C. Challenges in Implementing Cybersecurity Frameworks in Higher Education Institutions

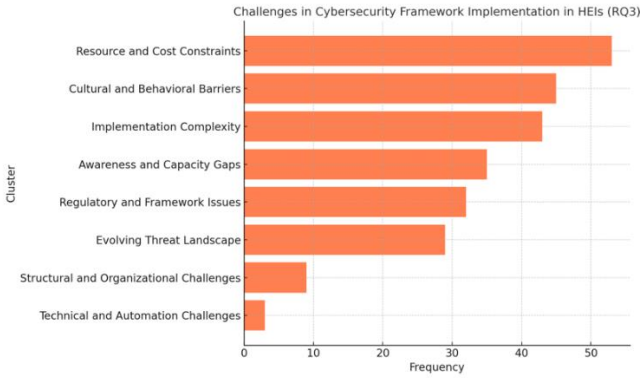
The third research question explored the challenges faced by HEIs in implementing cybersecurity frameworks. The 14 identified themes were grouped into eight categories, offering a structured view of recurring barriers.

The most significant cluster was Resource and Cost Constraints, mentioned in 53 instances, highlighting funding limitations, ROI concerns, and workforce shortages. These challenges were followed by Implementation Complexity (45 mentions), which included integration barriers and system-level complexities within HEIs.

As cited in 45 studies, cultural and behavioral barriers point to resistance to change and inconsistent stakeholder engagement. The Evolving Threat Landscape cluster, with 29 mentions, emphasizes the need to adapt continuously to new and dynamic security risks.

Thematic challenges such as the Awareness and Capacity Gaps (35 mentions) and Regulatory and Framework Issues (32 mentions) reflected knowledge deficits, policy confusion, and overlapping standards. Lesser but still critical were Structural and Organizational Challenges (9 mentions) and Technical and Automation Challenges (3 mentions), which included issues like decentralization and documentation limitations. These results reinforce the need for comprehensive planning that addresses technical readiness, institutional culture, and resource allocation. Figure 4 presents the distribution of implementation challenges of the cybersecurity framework identified in the reviewed studies.

Figure 4. Challenges in Implementing Cybersecurity Frameworks in Higher Education Institutions



The findings of this systematic literature review provide meaningful insights into the current state of cybersecurity frameworks in the context of HEIs. The characteristics identified, particularly adaptability, comprehensiveness, and alignment with institutional governance, affirm the necessity of flexible and scalable frameworks to fit the distinct academic environment. These align with [5] and [38], which emphasized the dynamic nature of HEI ecosystems and the importance of continuous adaptation.

The study also reinforces the centrality of risk management, awareness training, and compliance mechanisms as foundational components. These mirror the critical success factors proposed in general cybersecurity literature [36][30]. Yet, the contextual demands of HEIs—such as open-access culture, diverse stakeholders, and decentralized IT structures—require that these components be reinterpreted for educational contexts. This position supports the argument that frameworks developed for corporate use often fall short in addressing the nuanced operational realities of HEIs [15].

Received: August 08, 2025

Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The documented challenges, including resource constraints, cultural resistance, and the evolving threat landscape, suggest that implementation difficulties persist even when frameworks are in place. These reflect persistent capacity gaps noted in literature from developed and developing contexts [14][40]. Regulatory fragmentation and lack of standardization further compound these issues, calling for sector-specific policy reforms and localized adaptation of global standards.

Notably, the geographical and methodological distribution of studies reviewed in this SLR underscores a growing global awareness of cybersecurity issues in HEIs. However, the relative scarcity of quantitative validation studies and implementation-focused assessments indicates an ongoing need for empirical testing of proposed frameworks in real-world HEI environments.

Conclusion and Recommendation

This systematic literature review synthesized cybersecurity-related studies spanning 2010 to 2024, focusing on characteristics, components, and challenges associated with frameworks for higher education institutions. The findings indicate that while existing frameworks offer a solid foundation, their adaptation to the HEI context is limited by a lack of cultural fit, implementation complexity, and resource constraints.

HEIs are encouraged to 1) prioritize comprehensive, adaptable, and user-centric cybersecurity frameworks tailored to academic environments; 2. institutionalize continuous improvement processes and regular risk assessments as standard practice; 3. invest in awareness and training programs to build a security-conscious culture; and 4. advocate for harmonized cybersecurity regulations and localized standards that reflect the educational mission and structural realities of HEIs.

Future research should focus on empirically validating proposed frameworks in diverse academic settings, including small, resource-limited HEIs. Additionally, longitudinal studies assessing framework maturity and effectiveness over time could offer deeper insights into implementation outcomes.

This study provides foundational guidance for cybersecurity planners and policymakers in higher education. It offers a structured roadmap to guide the development, evaluation, and refinement of cybersecurity strategies within the academic sector.

Supplementary Material

Note: Due to space limitations of the publication format, supplementary materials (e.g., detailed tables, figures, and appendices) have not been included in this manuscript. These materials, including the full evaluation instrument, consolidated matrices, and illustrative outputs, are available upon request from the corresponding author.

REFERENCES

[1] J. Jang-Jaccard and S. Nepal, “A survey of emerging threats in cybersecurity,” *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, Aug. 2014, doi: 10.1016/j.jcss.2014.02.005.

[2] C. L. Stevenson, “To choose a definition is to plead a cause.,” 2014.

[3] R. K. Goutam, “Importance of Cyber Security,” *Int. J. Comput. Appl.*, vol. 111, no. 7, 2015.

Received: August 08, 2025

Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[4] I. Atoum, A. Otoom, and A. Abu Ali, "A holistic cyber security implementation framework," *Inf. Manag. Comput. Secur.*, vol. 22, no. 3, pp. 251–264, Jul. 2014, doi: 10.1108/IMCS-02-2013-0014.

[5] R. Azmi, W. Tibben, and K. T. Win, "Review of cybersecurity frameworks: context and shared concepts," *J. Cyber Policy*, vol. 3, no. 2, pp. 258–283, May 2018, doi: 10.1080/23738871.2018.1520271.

[6] A. M. Rea-Guaman, J. Mejía, T. San Feliu, and J. A. Calvo-Manzano, "AVARCIBER: a framework for assessing cybersecurity risks," *Clust. Comput.*, vol. 23, no. 3, pp. 1827–1843, Sep. 2020, doi: 10.1007/s10586-019-03034-9.

[7] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Comput. Secur.*, vol. 92, p. 101747, May 2020, doi: 10.1016/j.cose.2020.101747.

[8] P. Kuppusamy *et al.*, "Systematic Literature Review of Information Security Compliance Behaviour Theories," *J. Phys. Conf. Ser.*, vol. 1551, no. 1, p. 012005, May 2020, doi: 10.1088/1742-6596/1551/1/012005.

[9] V. Troia, G. Bottomly, S. Braxton-Lieber, J. Vucetic, and R. Capron, "THE CYBERSECURITY FRAMEWORK AS AN EFFECTIVE INFORMATION SECURITY BASELINE: A QUALITATIVE EXPLORATION," 2018.

[10] S. Krenn, "Cross Sectoral Cybersecurity Building Blocks," CyberSec4Europe Consortium, 2020.

[11] S. M. Alhidaifi, M. R. Asghar, and I. S. Ansari, "A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions," *ACM Comput. Surv.*, vol. 56, no. 8, pp. 1–48, Aug. 2024, doi: 10.1145/3649218.

[12] S. Mahmood, M. Chadhar, and S. Firmin, "Digital resilience framework for managing crisis: A qualitative study in the higher education and research sector," *J. Contingencies Crisis Manag.*, vol. 32, no. 1, p. e12549, Mar. 2024, doi: 10.1111/1468-5973.12549.

[13] J. B. Ulven and G. Wangen, "A Systematic Review of Cybersecurity Risks in Higher Education," *Future Internet*, vol. 13, no. 2, p. 39, Feb. 2021, doi: 10.3390/fi13020039.

[14] E. C. K. Cheng and T. Wang, "Institutional Strategies for Cybersecurity in Higher Education Institutions," *Information*, vol. 13, no. 4, p. 192, Apr. 2022, doi: 10.3390/info13040192.

[15] A. B. Nassoura, "Cybersecurity Technologies And Practices In Higher Education Institutions: A Systematic Review," vol. 19, no. 3, 2022.

[16] D. S. Butcher *et al.*, "Cybersecurity in a Large-Scale Research Facility—One Institution's Approach," *J. Cybersecurity Priv.*, vol. 3, no. 2, pp. 191–208, May 2023, doi: 10.3390/jcp3020011.

[17] I. Bongiovanni, "The least secure places in the universe? A systematic literature review on information security management in higher education," *Comput. Secur.*, vol. 86, pp. 350–357, Sep. 2019, doi: 10.1016/j.cose.2019.07.003.

[18] A. M. Amine, E. M. Chakir, T. Issam, and Y. I. Khamlichi, "A Review of Cybersecurity Management Standards Applied in Higher Education Institutions," *Int. J. Saf. Secur. Eng.*, vol. 13, no. 6, pp. 1109–1116, Dec. 2023, doi: 10.18280/ijsse.130614.

[19] L. Coleman and B. M. Purcell, "Data Breaches in Higher Education," vol. 15, 2015.

Received: August 08, 2025

[20] A. N. Ahmadi, "A COMPREHENSIVE CYBERSECURITY FRAMEWORK FOR AFGHANISTAN'S CYBERSPACE," *Int. J. Eng. Appl. Sci. Technol.*, vol. 6, no. 2, Jun. 2021, doi: 10.33564/IJEAST.2021.v06i02.032.

[21] M. A. Mohamed Hashim, I. Tlemsani, and R. Matthews, "Higher education strategy in digital transformation," *Educ. Inf. Technol.*, vol. 27, no. 3, pp. 3171–3195, Apr. 2022, doi: 10.1007/s10639-021-10739-1.

[22] M. A. Haque *et al.*, "Cybersecurity in Universities: An Evaluation Model," *SN Comput. Sci.*, vol. 4, no. 5, p. 569, Jul. 2023, doi: 10.1007/s42979-023-01984-x.

[23] K. Alshammari, T. Beach, Y. Rezgui, and R. Alelwani, "Built Environment Cybersecurity: Development and Validation of a Semantically Defined Access Management Framework on a University Case Study," *Appl. Sci.*, vol. 13, no. 13, p. 7518, Jun. 2023, doi: 10.3390/app13137518.

[24] C. E. Bondoc and T. G. Malawit, "Cybersecurity for higher education institutions: adopting regulatory framework," *Glob. J. Eng. Technol. Adv.*, vol. 2, no. 3, pp. 016–021, Mar. 2020, doi: 10.30574/gjeta.2020.2.3.0013.

[25] S. Yusif and A. Hafeez-Baig, "Cybersecurity Policy Compliance in Higher Education: A Theoretical Framework," *J. Appl. Secur. Res.*, vol. 18, no. 2, pp. 267–288, Apr. 2023, doi: 10.1080/19361610.2021.1989271.

[26] M. Syafrizal, S. R. Selamat, and N. A. Zakaria, "Analysis of Cybersecurity Standard and Framework Components," *Int. J. Commun. Netw. Inf. Secur. IJCNIS*, vol. 12, no. 3, Apr. 2022, doi: 10.17762/ijcnis.v12i3.4817.

[27] H. Taherdoost, "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," *Electronics*, vol. 11, no. 14, p. 2181, Jul. 2022, doi: 10.3390/electronics11142181.

[28] G. M. Nist, "The NIST Cybersecurity Framework 2.0," National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, 2023. doi: 10.6028/NIST.CSWP.29.

[29] M. A. Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency," *Procedia Comput. Sci.*, vol. 161, pp. 1206–1215, 2019, doi: 10.1016/j.procs.2019.11.234.

[30] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS," *JOIV Int. J. Inform. Vis.*, vol. 4, no. 4, pp. 225–230, Dec. 2020, doi: 10.30630/joiv.4.4.482.

[31] A. Tolah, S. M. Furnell, and M. Papadaki, "An empirical analysis of the information security culture key factors framework," *Comput. Secur.*, vol. 108, p. 102354, Sep. 2021, doi: 10.1016/j.cose.2021.102354.

[32] W. Yeoh, S. Wang, A. Popovič, and N. H. Chowdhury, "A systematic synthesis of critical success factors for cybersecurity," *Comput. Secur.*, vol. 118, p. 102724, Jul. 2022, doi: 10.1016/j.cose.2022.102724.

[33] P. Cheimonidis and K. Rantos, "Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review," *Future Internet*, vol. 15, no. 10, p. 324, Sep. 2023, doi: 10.3390/fi15100324.

Received: August 08, 2025

Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[34] I. Almomani, M. Ahmed, and L. Maglaras, "Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia," *PeerJ Comput. Sci.*, vol. 7, p. e703, Sep. 2021, doi: 10.7717/peerj-cs.703.

[35] K. Al Harthy, F. Al Shuhaimi, and K. K. Juma Al Ismaily, "The upcoming Blockchain adoption in Higher-education: requirements and process," in *2019 4th MEC International Conference on Big Data and Smart City (ICBDSC)*, Muscat, Oman: IEEE, Jan. 2019, pp. 1–5. doi: 10.1109/ICBDSC.2019.8645599.

[36] A. Aliyu *et al.*, "A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom," *Appl. Sci.*, vol. 10, no. 10, p. 3660, May 2020, doi: 10.3390/app10103660.

[37] M. Angelini, S. Lenti, and G. Santucci, "CRUMBS: A cyber security framework browser," in *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Phoenix, AZ, USA: IEEE, Oct. 2017, pp. 1–8. doi: 10.1109/VIZSEC.2017.8062194.

[38] A. Asmawati, N. Hermawati, C. T. Karisma, D. Ayu, A. I. Setyobudi, and M. A. Alyano, "SmartPLS Application for Evaluating Cybersecurity Resilience in University of Raharja IT Infrastructure," *Int. J. Cyber IT Serv. Manag.*, vol. 4, no. 1, pp. 1–10, Feb. 2024, doi: 10.34306/ijcitsm.v4i1.141.

[39] A. Alexei, "Implementing Design Science Research Method to Develop a Cyber Security Framework for HEIs in Moldova," in *Proceedings of the 11th International Conference on "Electronics, Communications and Computing (IC|ECCO-2021),"* Technical University of Moldova, Apr. 2022, pp. 228–231. doi: 10.52326/ic-ecco.2021/NWC.02.

[40] A. Arista and K. N. M. Ngafidin, "An Information System Risk Management of a Higher Education Computing Environment," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 12, no. 2, p. 557, Apr. 2022, doi: 10.18517/ijaseit.12.2.13953.

[41] B. Badamasi and S. C. A. Utulu, "FRAMEWORK FOR MANAGING CYBERCRIME RISKS IN NIGERIAN UNIVERSITIES," 2021.

[42] A. Alenezi, "Cybersecurity risks and strategies in learning services of Higher Education Institutions (HEIs) in developing and emerging countries – a critical scoping review," *Egypt. J. Bus. Stud.*, vol. 48, no. 3, pp. 480–506, Jul. 2024, doi: 10.21608/alat.2024.373548.

[43] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: Systematic review," *Comput. Secur.*, vol. 99, p. 102030, Dec. 2020, doi: 10.1016/j.cose.2020.102030.

[44] D. Anderson, O. P. Abiodun, and A. Christoffels, "Information security at South African universities—implications for biomedical research," *Int. Data Priv. Law*, vol. 10, no. 2, pp. 180–186, May 2020, doi: 10.1093/idpl/ipaa007.

[45] A. Alexei, "CYBER SECURITY STRATEGIES FOR HIGHER EDUCATION INSTITUTIONS," *J. Eng. Sci.*, vol. XXVIII, no. 4, pp. 74–92, Dec. 2021, doi: 10.52326/jes.utm.2021.28(4).07.

[46] B. Mtakati and F. Sengati, "Cybersecurity Posture of Higher Learning Institutions in Tanzania," *J. Inform.*, vol. 1, no. 1, Mar. 2021, doi: 10.59645/tji.v1i1.1.

[47] J. S. Bissumbhar, "The Cyber Shield: Uniting Forces for Knowledge Security in Universities," Delft University of Technology, 2023.

Received: August 08, 2025

[48] H. Chen and Zhenying Hu, "Exploring Data Traceability Methods in Information Management Within Universities: An Action Research and Case Study Approach," *IEEE Access*, vol. 12, pp. 175196–175217, 2024, doi: 10.1109/ACCESS.2024.3493860.

[49] J. Christopher, G. Jung, and C. Doane, "Making it More Secure: The Technical and Social Challenges of Expanding the Functionality of an Existing HPC Cluster to Meet University and Federal Data Security Requirements," in *Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (learning)*, Chicago IL USA: ACM, Jul. 2019, pp. 1–5. doi: 10.1145/3332186.3332250.

[50] N. M. De Ramos and F. D. Esponilla Ii, "Cybersecurity program for Philippine higher education institutions: A multiple-case study," *Int. J. Eval. Res. Educ. IJERE*, vol. 11, no. 3, p. 1198, Sep. 2022, doi: 10.11591/ijere.v11i3.22863.

[51] A. Dedeke and K. Masterson, "Contrasting cybersecurity implementation frameworks (CIF) from three countries," *Inf. Comput. Secur.*, vol. 27, no. 3, pp. 373–392, Jul. 2019, doi: 10.1108/ICS-10-2018-0122.

[52] B. M. Dioubate and W. N. Wan Daud, "A Review of Cybersecurity Risk Management Framework in Malaysia Higher Education Institutions," *Int. J. Acad. Res. Bus. Soc. Sci.*, vol. 12, no. 5, p. Pages 1081-1093, May 2022, doi: 10.6007/IJARBSS/v12-i5/12924.

[53] A. Y. Eshetu, E. A. Mohammed, and A. O. Salau, "Cybersecurity vulnerabilities and solutions in Ethiopian university websites," *J. Big Data*, vol. 11, no. 1, p. 118, Aug. 2024, doi: 10.1186/s40537-024-00980-z.

[54] S. M. Furnell *et al.*, "A security framework for online distance learning and training," *Internet Res.*, vol. 8, no. 3, pp. 236–242, Aug. 1998, doi: 10.1108/10662249810217821.

[55] A. A. Garba and A. M. Bade, "An Investigation on Recent Cyber Security Frameworks as Guidelines for Organizations Adoption," vol. 6, no. 2, 2021.

[56] H. Balhareth, "CLOUD COMPUTING STRATEGY AND ADOPTION IN HIGHER EDUCATION: THE CASE OF SAUDI ARABIA," *Int. J. Inf. Technol. Manag. Inf. Syst.*, vol. 9, no. 1, Mar. 2018, doi: 10.34218/IJITMIS.9.1.2018.003.

[57] S. Hina and P. D. D. Dominic, "Information security policies' compliance: a perspective for higher education institutions," *J. Comput. Inf. Syst.*, vol. 60, no. 3, pp. 201–211, May 2020, doi: 10.1080/08874417.2018.1432996.

[58] I. Atoum and A. Otoom, "A Classification Scheme for Cybersecurity Models," *Int. J. Secur. Its Appl.*, vol. 11, no. 1, pp. 109–120, Jan. 2017, doi: 10.14257/ijsia.2017.11.1.10.

[59] Izzah Inani Abdul Halim, Alya Geogiana Buja, Mohd Shah Shafie Idris, and Nurul Jannah Mahat, "Implementation of BYOD Security Policy in Malaysia Institutions of Higher Learning (MIHL): An Overview," *J. Adv. Res. Appl. Sci. Eng. Technol.*, vol. 33, no. 2, pp. 1–14, Nov. 2023, doi: 10.37934/araset.33.2.114.

[60] J. W. Coffey, M. Haveard, and G. Golding, "A Case Study in the Implementation of a Human-Centric Higher Education Cybersecurity Program," *J. Cybersecurity Educ. Res. Pract.*, vol. 2018, no. 1, Jul. 2018, doi: 10.62915/2472-2707.1028.

[61] C. M. Kang, P. S. JosephNg, and K. Issa, "A Study on Integrating Penetration Testing into the Information Security Framework for Malaysian Higher Education Institutions," presented at the 2015 International Symposium on Mathematical Sciences and Computing Research (iSMCS), 2015, pp. 156–161.

Received: August 08, 2025

[62] K. Kepuska and M. Tomasevic, "A lightweight framework for cyber risk management in Western Balkan higher education institutions," *PeerJ Comput. Sci.*, vol. 10, p. e1958, Apr. 2024, doi: 10.7717/peerj-cs.1958.

[63] A. D. Khaleefah and H. M. Al-Mashhadi, "Methodologies, Requirements, and Challenges of Cybersecurity Frameworks: A Review," *Iraqi J. Sci.*, pp. 468–486, Jan. 2024, doi: 10.24996/ijs.2024.65.1.38.

[64] A. Kumar, K. Mishra, R. Kumar Mahto, and B. Kumar Mishra, "A Framework for Institution to Enhancing Cybersecurity in Higher Education: A Review," *LatIA*, vol. 2, p. 94, Jan. 2024, doi: 10.62486/latia202494.

[65] H. S. Lallie, A. Thompson, E. Titis, and P. Stephens, "Understanding Cyber Threats Against the Universities, Colleges, and Schools," Jul. 15, 2023, *arXiv*: arXiv:2307.07755. Accessed: Sep. 27, 2024. [Online]. Available: http://arxiv.org/abs/2307.07755

[66] B. Irvin Lamarca, "Cybersecurity Risk Assessment of the University of Northern Philippines using PRISM Approach," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 769, no. 1, p. 012066, Feb. 2020, doi: 10.1088/1757-899X/769/1/012066.

[67] M. Dawson, "Applying a holistic cybersecurity framework for global IT organizations," *Bus. Inf. Rev.*, vol. 35, no. 2, pp. 60–67, Jun. 2018, doi: 10.1177/0266382118773624.

[68] J. Merchan-Lima, F. Astudillo-Salinas, L. Tello-Oquendo, F. Sanchez, G. Lopez-Fonseca, and D. Quiroz, "Information security management frameworks and strategies in higher education institutions: a systematic review," *Ann. Telecommun.*, vol. 76, no. 3–4, pp. 255–270, Apr. 2021, doi: 10.1007/s12243-020-00783-2.

[69] M. H. Suwito, S. Matsumoto, J. Kawamoto, D. Gollmann, and K. Sakurai, "An Analysis of IT Assessment Security Maturity in Higher Education Institution," in *Information Science and Applications (ICISA) 2016*, vol. 376, K. J. Kim and N. Joukov, Eds., in Lecture Notes in Electrical Engineering, vol. 376. , Singapore: Springer Singapore, 2016, pp. 701–713. doi: 10.1007/978-981-10-0557-2_69.

[70] O. W. Adejo, I. Ewuzie, A. Usoro, and T. Connolly, "E-Learning to m-Learning: Framework for Data Protection and Security in Cloud Infrastructure," *Int. J. Inf. Technol. Comput. Sci.*, vol. 10, no. 4, pp. 1–9, Apr. 2018, doi: 10.5815/ijitcs.2018.04.01.

[71] X. Olsen, "Enterprise purple teaming: An exploratory qualitative study," Dissertation, Marymount University, 2022.

[72] Nancy Plumer, "Cybersecurity Maturity Assessment: Integrating IAM in Zero Trust Model for Peruvian Universities," Saint Thomas University, Miami, Florida, 2024.

[73] S. Salagrama, "An Effective Design of Model for Information Security Requirement Assessment," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 10, 2021, doi: 10.14569/IJACSA.2021.0121001.

[74] S. Almuhammadi and M. Alsaleh, "Information Security Maturity Model for Nist Cyber Security Framework," in *Computer Science & Information Technology (CS & IT)*, Academy & Industry Research Collaboration Center (AIRCC), Feb. 2017, pp. 51–62. doi: 10.5121/csit.2017.70305.

[75] R. Villalón-Fonseca, "The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity," *Comput. Secur.*, vol. 120, p. 102805, Sep. 2022, doi: 10.1016/j.cose.2022.102805.

Received: August 08, 2025

Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[76] W. Yustanti, A. Qoiriah, R. Bisma, and A. Pri Hanto, "An analysis of Indonesia's information security index: a case study in a public university," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 296, p. 012038, Jan. 2018, doi: 10.1088/1757-899X/296/1/012038.

[77] J. Webb and D. Hume, "Campus IoT Collaboration and Governance using the NIST Cybersecurity Framework," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, London, UK: Institution of Engineering and Technology, 2018, p. 25 (7 pp.)-25 (7 pp.). doi: 10.1049/cp.2018.0025.

[78] S. Xu, "The Cybersecurity Dynamics Way of Thinking and Landscape," in *Proceedings of the 7th ACM Workshop on Moving Target Defense*, Virtual Event USA: ACM, Nov. 2020, pp. 69–80. doi: 10.1145/3411496.3421225.

[79] Z. Ismail, M. Masrom, Z. Sidek, and D. Hamzah, "Framework to Manage Information Security for Malaysian Academic Environment," *J. Inf. Assur. Cybersecurity*, pp. 1–16, Jan. 2010, doi: 10.5171/2010.305412.

Received: August 08, 2025