Comparative Analysis of Cybersecurity Frameworks in Educational Institutions: Towards a Tailored Security Model

Syarif Hidayatulloh[1], Aedah Binti Abd. Rahman[2]
Department of Informatics Engineering, Adhirajasa Reswara Sanjaya University, Bandung, Indonesia[1]
Department of School of Science and Technology, Asia e University, Kuala Lumpur, Malaysia[2]

***Abstract*—Educational institutions face unique cybersecurity challenges due to their open culture, decentralised structures, and limited resources. While standard frameworks such as NIST, ISO/IEC 27001, and COBIT offer comprehensive guidance, their full implementation in academic settings is often impractical. This study addresses the gap by conducting a document-based comparative analysis of these frameworks, focusing on their applicability in educational institutions. A total of 42 documents—including case studies, cybersecurity guidelines, and academic articles—were analysed using thematic coding. The findings reveal significant misalignments between current frameworks and academic environments, particularly in terms of complexity, adaptability, and resource demand. Based on these insights, a tailored cybersecurity model is proposed. The model emphasises modularity, cultural integration, resource optimisation, and decentralised implementation to suit the educational context. A multi-step validation plan is also outlined to assess the model's practicality. This research offers both theoretical and practical contributions to cybersecurity governance in the education sector.**

***Keywords*—Cybersecurity; educational institutions; cybersecurity frameworks; tailored security model**

I. Introduction

Cybersecurity is increasingly critical for educational institutions as they rely heavily on digital technologies for managing student data and facilitating learning. The shift towards digital transformation, accelerated by the COVID-19 pandemic, has heightened vulnerabilities to cyberattacks, including ransomware incidents that disrupt educational processes and compromise sensitive data [1], [2], [26]. Integrating digital tools in education must be accompanied by robust cybersecurity measures to protect against threats such as data breaches and privacy violations [3], [4]. Furthermore, educational leaders play a vital role in fostering a culture of cybersecurity awareness among staff and students, ensuring they are equipped to navigate the digital landscape safely [5], [6]. Comprehensive training and resources are paramount, as many educators may lack the necessary skills to manage cybersecurity risks effectively [7], [8].

The cybersecurity landscape within educational institutions is fraught with challenges, despite an increasing recognition of its importance. Many institutions, from primary schools to universities, face significant deficiencies in their cybersecurity frameworks. Key factors contributing to this vulnerability include budget constraints, which limit the ability to invest in robust security systems, and a pervasive lack of awareness regarding the risks associated with cyber threats [1], [2]. Furthermore, insufficient resources hinder the implementation of adequate security measures, leaving institutions exposed to potential cyberattacks, such as ransomware incidents that have disrupted educational processes and compromised sensitive data [3], [4]. The reliance on digital technology for managing student information and internal communications amplifies these risks, necessitating a proactive approach to cybersecurity that includes training, awareness campaigns, and investment in protective technologies [5],[6]. Addressing these challenges is critical for safeguarding the integrity of educational environments in an increasingly digital world.

Cybersecurity frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001 have been widely adopted across various sectors to safeguard data and infrastructure against cyber threats. However, their application within educational institutions often reveals significant shortcomings, primarily due to the unique environment of openness and collaboration, which simultaneously increases cyberattack vulnerabilities [9]. This necessitates the development of a tailored security model specifically designed for the educational sector, addressing its distinct needs and challenges [10].

A comparative analysis of existing frameworks indicates that while they provide foundational guidelines, they may not fully encompass the specific operational realities of educational institutions [11]. For instance, integrating cybersecurity education into curricula is essential for fostering awareness among students and staff, yet many institutions struggle with inadequate resources and training programs [12], [13], [47]. By identifying the weaknesses in current frameworks and proposing a more suitable model, this research aims to enhance the cybersecurity posture of educational institutions, ultimately contributing to more effective cybersecurity policies and practices [14]. The findings are expected to serve as a valuable resource for policymakers and practitioners in designing targeted security measures that align with the unique demands of the education sector [15].

As digital transformation accelerates in the education sector, the danger of cyberattacks, such as ransomware and data breaches, becomes increasingly evident. Educational institutions, from K-12 schools to major universities, often lack the technical, financial, and organisational capacity to fully implement standard cybersecurity frameworks. Instead, they need flexible solutions that suit their distinct operational structures and resource constraints.

This study critically examines three widely adopted frameworks: NIST Cybersecurity Framework, ISO/IEC 27001, and COBIT, assessing their suitability for educational settings. Based on an extensive literature review and qualitative document analysis, the study introduces a customised cybersecurity model. Consequently, this research contributes to both academic and practical fields by proposing a tailored cybersecurity framework suited to the educational environment.

The remainder of this study is organised as follows:

Section II reviews the literature on existing cybersecurity frameworks—particularly NIST, ISO/IEC 27001, and COBIT—and discusses their applicability and limitations within educational institutions.

Section III describes the research methodology, detailing the qualitative document analysis approach and data sources used to evaluate the frameworks

Section IV presents the comparative analysis results, identifies key implementation challenges, and synthesises findings to support the development of a tailored model

Section V proposes the customised cybersecurity model, explains its five core components, and discusses its practical implications for educational policy and governance.

Section VI concludes the study by summarising the main contributions, outlining limitations, and offering recommendations for future research and validation.

II. Literature Review

A. *Overview of Cybersecurity Frameworks*

Cybersecurity frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, and COBIT offer comprehensive guidelines for managing cybersecurity risks. These frameworks are frequently utilised in corporate sectors but encounter difficulties in educational settings.

The NIST Cybersecurity Framework is built around five core functions: Identify, Protect, Detect, Respond, and Recover. This framework enables organisations to comprehensively understand their cybersecurity posture and effectively implement strategies to manage risks [1].

ISO/IEC 27001 focuses on information security management, systematically safeguarding sensitive organisational information. It establishes requirements for an Information Security Management System (ISMS), ensuring that information security is integrated into the organisation's overall management processes [2].

COBIT (Control Objectives for Information and Related Technologies) provides a framework for IT governance and management. It ensures that IT risks are effectively managed while supporting the achievement of organisational goals. It emphasises aligning IT and business objectives, enhancing overall governance [3].

These frameworks collectively contribute to a robust cybersecurity strategy, enabling organisations to navigate the complexities of the digital landscape.

B. *Application in Educational Institutions*

Implementing cybersecurity frameworks in educational institutions presents unique challenges due to their inherent culture of openness and collaboration. While frameworks like the NIST Cybersecurity Framework and ISO/IEC 27001 are widely adopted across various sectors, their application in academia often encounters difficulties. For example, the NIST Cybersecurity Framework, which emphasises five core functions—Identify, Protect, Detect, Respond, and Recover—has proven valuable in raising awareness and improving responses to cyber incidents in educational environments. However, it often falls short in addressing specific academic needs, such as protecting sensitive research data and ensuring student privacy [16],[17].

Similarly, while ISO/IEC 27001 offers a strong framework for information security management, its implementation in educational institutions can be limited by resource shortages and a lack of technical skills among staff [17]. Comparable challenges have been seen in non-educational sectors trying hybrid models [34]. Open access policies and looser controls over campus devices further increase vulnerabilities, making it easier for cybercriminals to target these weaknesses [18],[19]. Consequently, there is an urgent need for a customised cybersecurity model that reflects the specific operational realities of educational institutions, improving their capacity to safeguard sensitive data and counter cyber threats effectively [20],[21],[32].

Although these frameworks are beneficial, their inflexible structures and significant resource demands make them challenging to implement in schools and universities with limited budgets and decentralised systems.

C. *Challenges and Gaps*

Implementing cybersecurity frameworks in educational institutions, especially at the K-12 level, encounters significant challenges mainly due to resource limitations and cultural resistance to change. Many institutions operate with tight budgets that restrict their ability to adopt and implement all recommended controls from established frameworks like the NIST Cybersecurity Framework and ISO/IEC 27001. This financial constraint is further compounded by a shortage of IT staff with specialised cybersecurity skills, which can impede the practical application of these frameworks, even when they are adopted.

Cultural resistance to change further complicates the situation. Educational institutions often emphasise academic freedom and open access, which can conflict with strict cybersecurity measures that require tight access controls and monitoring of system usage. This tension between the need for strong cybersecurity and the desire to maintain an open, collaborative academic environment creates a challenging landscape for administrators responsible for protecting digital infrastructure. Therefore, addressing these challenges demands a nuanced approach that balances security requirements with the core values of educational institutions.

Key barriers include:

- High complexity and implementation cost, and inconsistent use of standard risk analysis methods across institutions [27].
- Misalignment with the academic culture
- Shortage of skilled IT personnel
- Decentralised decision-making structures

D. Previous Research Findings

Previous studies highlight the necessity for a more flexible, education-specific cybersecurity framework. However, few have presented practical models customised for the educational setting.

Previous research emphasises an urgent need to adapt established cybersecurity frameworks such as NIST and ISO/IEC 27001 to better suit educational contexts. Studies show that many academic institutions often adopt only parts of these frameworks due to budget limitations and a lack of specialised expertise [22]. This partial implementation highlights the necessity for a more flexible and adaptable framework that can be customised to the specific resources and needs of educational settings [23].

Furthermore, research highlights the advantages of developing a cybersecurity framework specifically designed for educational institutions. Such a customised framework can better address unique challenges, such as protecting student data and maintaining academic freedom, compared to the generic "one-size-fits-all" approaches of existing frameworks [24]. By focusing on the specific characteristics of educational institutions, a personalised framework could enhance cybersecurity preparedness and resilience, ultimately offering stronger protection against cyber threats [25].

III. Research Methodology

A. Research Design

The research methodology for this study adopts a qualitative approach, primarily using document analysis as the main method for data collection and analysis. This approach effectively investigates how various cybersecurity frameworks are adopted within educational institutions, enabling a detailed examination of the challenges and weaknesses faced during their implementation. Document analysis allows for the review of published policies, research reports, and relevant case studies, providing valuable insights into current practices and highlighting potential areas for further improvement.

Previous research has underscored the significance of customising cybersecurity frameworks to fit the particular context of educational institutions. For example, it highlights the need to understand the components of cybersecurity standards and frameworks to guide future research. Furthermore, it reviews the key factors that influence the implementation of information security management systems, which are important when assessing educational settings. Analysing these documents helps to identify the unique challenges faced by educational institutions in adopting frameworks such as NIST and ISO/IEC 27001, ultimately assisting in the development of a tailored cybersecurity model that addresses their specific needs.

B. Data Collection Method: Document Analysis

Document analysis serves as the primary data collection method for this study. The documents analysed include various sources such as:

- Cybersecurity Policy Reports: Reports published by educational institutions, government agencies, and non-governmental organisations focusing on implementing cybersecurity in the education sector.
- Case Studies: Published case studies on the implementation of cybersecurity frameworks in various educational institutions worldwide, providing empirical data on the effectiveness and challenges of these frameworks.
- Journal and Conference Articles: Peer-reviewed academic articles discussing the implementation of cybersecurity frameworks in educational settings and providing critical assessments of their suitability, as well as reviews of ICT tools used in higher education [46].
- Cybersecurity Standards and Guidelines: Official documents detailing standards and guidelines such as the NIST Cybersecurity Framework, ISO/IEC 27001, and COBIT and how these standards are adapted or used in educational institutions.

The data collection process through document analysis involves several key steps:

- Identification of Documents: Relevant documents were identified through searches in academic databases such as Scopus, IEEE Xplore, and Google Scholar, as well as through the websites of related organisations like NIST and ISO.
- Document Selection: Documents were selected based on relevance, reliability, and coverage. Documents specifically focused on the education sector or providing a critical evaluation of cybersecurity framework implementation were considered primary sources.
- Data Extraction: Key information from each document was extracted and organised based on the identified themes, such as framework effectiveness, implementation challenges, and adaptation for educational environments.

A total of 42 documents were examined in this study, chosen for their relevance, reliability, and direct link to cybersecurity in educational institutions. The distribution of documents is presented in Table I.

TABLE I. DOCUMENT AND SELECTION OVERVIEW

Document Type	Number	Source	Selection Criteria
Cybersecurity Policy Reports	10	Institutional & government sites	Targeting education sector; policy focus
Case Studies	8	Journals, conferences	Practical application of NIST, ISO/IEC 27001, or COBIT
Journal Articles	20	Scopus, IEEE Xplore, Google Scholar	Peer-reviewed, published 2018 or later
Framework Guidelines	4	NIST, ISO, ISACA	Descriptions of CSF, ISMS, and COBIT frameworks

C. Data Analysis

Document analysis was performed manually employing thematic coding grounded in principles of grounded theory. The procedure involved these steps:

1) Initial reading: Documents were read line by line to gain familiarity.

2) Open coding: Keywords and key ideas were extracted manually using Excel spreadsheets (no qualitative software used).

3) Axial coding: Categories were formed by linking similar open codes (e.g., "resource constraints", "training gaps").

4) Selective coding: Central themes such as "framework limitations" and "cultural mismatch" were identified.

The coding process and resulting categories are illustrated in Table II.

TABLE II. EXAMPLES OF CODE CATEGORIES AND THEMES

Open Code	Axial Category	Selective Theme
High cost of ISO adoption	Resource Limitation	Framework Limitations
Lack of IT staff	Resource Limitation	Framework Limitations
Decentralized departments	Governance Challenges	Cultural Misalignment
Need for open access	Academic Openness	Cultural Misalignment

This analysis provides a strong foundation for comparing different cybersecurity frameworks and evaluating their suitability for educational institutions. The results will be used to support the argument that a tailored cybersecurity model is explicitly needed for the education sector.

D. Research Workflow

The research process is summarized in Fig. 1, which illustrates the flow from literature review to framework synthesis and model development.

Fig. 1 illustrates the structured research design employed in this study, beginning with a literature review phase aimed at identifying existing cybersecurity frameworks and their known limitations in educational settings. This crucial step informed the subsequent document analysis, during which a selection of 42 documents, including policies, case studies, and academic research, were systematically examined using thematic coding techniques.

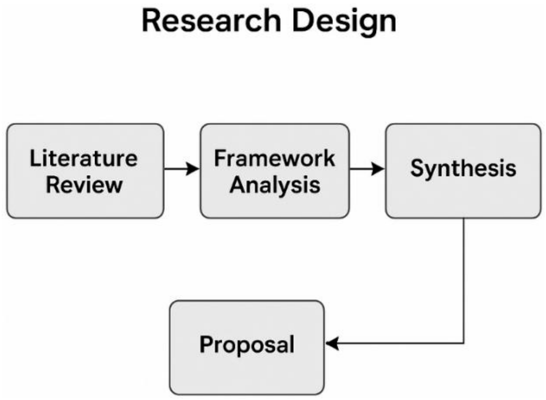

Fig. 1. Research design.

The insights gained from document analysis were then combined to identify common challenges and individual institutional needs. These findings were compared with key frameworks (NIST, ISO/IEC 27001, and COBIT) to highlight areas of misalignment, as shown in the figure.

Following this, the study moved on to the framework synthesis phase, where key insights were turned into a conceptual model specifically designed for the education sector. This iterative design phase focused on flexibility, contextual relevance, and feasibility.

Finally, the model was prepared for validation planning, including designing a pilot implementation strategy, conducting expert interviews, and performing document audits, ensuring the framework's applicability could be tested in real-world educational contexts.

In essence, Fig. 1 serves as a visual guide to the research process, emphasising the logical sequence and interaction between each phase from initial inquiry to framework development and planned validation.

IV. RESULTS

A. Comparative Analysis of Frameworks

The strengths and limitations of NIST, ISO/IEC 27001, and COBIT frameworks are compared in Table III, based on six key criteria relevant to the educational context.

TABLE III. COMPARATIVE ANALYSIS OF FRAMEWORKS

Criteria	NIST CSF	ISO/IEC 27001	COBIT
Scope	Risk management	ISMS	IT Governance
Complexity	High	High	Moderate
Suitability for Education	Partial	Partial	Limited
Adaptability	Flexible but needs expertise	Rigid	Moderately adaptable
Resource Requirement	High	High	Moderate
Academic Alignment	Limited	Limited	Limited

After conducting document analysis, including various cybersecurity frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, and COBIT, we found that while these frameworks offer comprehensive approaches to cybersecurity management, they often do not fully align with educational institutions' specific needs.

1) NIST Cybersecurity framework: This framework helps organisations understand and manage cybersecurity risks through five core functions: Identify, Protect, Detect, Respond, and Recover. However, it is sometimes too complex to fully implement in the educational context, particularly in institutions with limited resources like K-12 schools. Reports show that many academic institutions can only implement parts of this framework, especially those requiring lower technical and financial investment.

2) ISO/IEC 27001: This framework provides a highly structured approach to information security management, focusing on developing and maintaining an Information Security Management System (ISMS). Although it has been successfully adopted in various sectors, challenges occur when used in educational institutions, where decentralisation and a lack of specialised expertise in information security management pose significant barriers. Research also indicates that implementing ISO/IEC 27001 in the education sector often requires considerable adaptation, as not all recommended controls and policies are relevant or practical for academic environments.

3) COBIT: Focusing on IT governance, COBIT offers a useful framework for ensuring that IT risks are managed effectively and support the organisation's strategic aims. However, when applied in educational institutions, such as large universities with complex organisational structures, this framework often encounters difficulties in enforcing uniform policies across various departments and faculties. A study found that while COBIT provides strong guidance for IT governance, its implementation in academic environments is frequently hindered by resistance to change and cultural differences across departments.

B. *Identification of Key Gaps*

The comparative analysis reveals several key weaknesses in the existing cybersecurity frameworks when applied to educational institutions:

1) Complexity of implementation: Frameworks like NIST and ISO/IEC 27001 are often too complex to fully implement without a structured decision-making approach tailored for educational cybersecurity [28], particularly those with limited resources. These limitations mean that many schools can only adopt parts of these frameworks, ultimately leaving gaps in their protection.

2) Misalignment with academic culture: Many cybersecurity frameworks are designed for more structured and controlled corporate environments. However, educational institutions often have a more open and collaborative culture, which can conflict with the need for strict access controls and monitoring of system usage.

3) Lack of resources and expertise: Implementing frameworks like ISO/IEC 27001 requires significant human and financial resources, which educational institutions often lack. Additionally, the shortage of IT staff with specialised cybersecurity skills is a substantial barrier to practical implementation.

4) Decentralised organisational structure: Educational institutions, such as huge universities, often have decentralised organisational structures, with different departments having varying policies and technological needs. This makes it challenging to implement a uniform framework across the institution, as reaching a consensus on security policies and procedures can be difficult.

C. *Synthesis of Findings*

The results of this document analysis emphasise an urgent need to develop a cybersecurity model that better fits the specific requirements of educational institutions. This customised model should consider resource limitations, academic culture, and the unique organisational structures of educational institutions. Although frameworks like NIST, ISO/IEC 27001, and COBIT offer valuable guidance, there are emerging suggestions for sector-specific cybersecurity frameworks to reduce attacks [29], and further adaptation and personalisation are necessary for successful implementation in the education sector.

The synthesis of these findings suggests that a more modular and adaptable cybersecurity framework is required to address the varied needs of educational institutions. This framework should enable institutions to implement the most relevant security controls that match their capabilities, without strictly following all recommendations.

V. Discussion

A. *Interpretation of Results*

The comparative analysis results demonstrate that while cybersecurity frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, and COBIT provide a strong foundation for managing cybersecurity risks, they often do not fully meet the specific needs of educational institutions. The main barriers to applying these frameworks in the education sector are the complexity of implementation, misalignment with academic culture, lack of resources, and decentralised organisational structures.

One key finding from this study is that existing frameworks are too rigid and focused on industrial sectors. A more holistic cybersecurity strategy may help bridge this contextual gap [41], [42], where operational environments tend to be more structured and hierarchical. In contrast, educational institutions have different needs, including supporting academic freedom and interdepartmental collaboration, which often conflict with strict cybersecurity principles. Therefore, a customised model is required to balance the need for stringent security with the open and flexible environment of educational institutions.

B. *Proposing a Tailored Security Model*

The components of the proposed model are outlined in Table IV.

TABLE IV. COMPONENTS OF THE TAILORED CYBERSECURITY MODEL

Component	Description (Concise)	Key Benefit
Modular Architecture	Flexible modules based on institutional size and context	Scalable and customisable
Cultural Integration	Support open collaboration while maintaining access control	Preserves academic freedom
Resource Optimization	Focus on cost-effective tools and strategic prioritisation	Feasible within limited budgets
Decentralized Governance	Tailored policies for departments with coordinated oversight	Compatible with the academic structure
Emerging Tech Integration	Integrate AI/IoT for proactive security posture	Future-proof and proactive

Expanded Explanation:

1) Modular and flexible structure: Educational institutions vary significantly in size, budget, and IT capacity. A one-size-fits-all cybersecurity framework [39] is neither practical nor effective. This approach encourages modularity, allowing each institution to select and implement only the components relevant to their risk profile, maturity level, and resources. Such flexibility makes the model scalable and adaptable. Interactive tools and gamified learning environments have shown potential in improving engagement [35].

2) Integration with educational culture: Academic institutions value openness, collaboration, and autonomy. A fundamental cybersecurity culture at all levels of the institution can help reinforce these values safely [49]. Therefore, the cybersecurity framework must balance protection with freedom. It promotes policies that facilitate secure departmental cooperation and integrates cybersecurity education into the institutional culture while addressing human-centric factors such as awareness and behavioural hygiene [43], which can be further supported through active learning-based security training [30], fostering awareness and behavioural change among faculty, staff, and students..

3) Resource optimisation: Recognising the budgetary and staffing constraints faced by most educational institutions, the framework encourages cost-effective practices. It promotes the use of open-source or shared security tools, centralised support services where feasible, and risk-based prioritisation to ensure limited resources are allocated to the most vulnerable or impactful areas. Adaptive training models for end-users also support cost-effective implementation [44].

4) Decentralised implementation: Given the diversity of academic departments, a centralised, rigid policy often faces opposition. Instead, this approach supports decentralised implementation within a central guiding framework, allowing departments to develop context-specific solutions while aligning with overall institutional aims. This respects local autonomy whilst maintaining institutional coherence.

5) Emerging technology integration: To stay relevant amidst the changing threat landscape, the framework includes provisions for adopting new technologies such as Artificial Intelligence, Internet of Things (IoT), and real-time analytics. These features improve early detection, response, and adaptive resilience across the institution.

Together, these components tackle the challenges identified in the previous analysis and offer a practical route to improve cybersecurity preparedness in the education sector.

To address the unique cybersecurity challenges faced by educational institutions, including structural decentralisation, limited resources, and the need to preserve academic openness, this study developed a tailored cybersecurity framework. The framework was constructed based on the synthesis of findings from comparative analysis and thematic coding, resulting in a model that is both theoretically grounded and practically applicable across various educational contexts. As shown in Fig. 2, the proposed framework comprises five key components: Modular Architecture, Cultural Integration, Resource Optimisation, Decentralised Governance, and Emerging Technology Integration. These components work together to form a cohesive and adaptable strategy designed to enhance cybersecurity readiness within the academic environment.

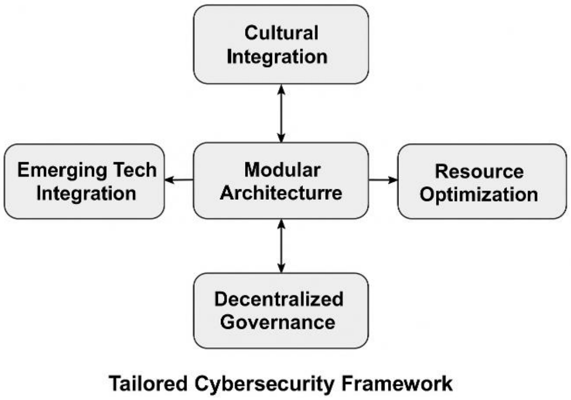

Fig. 2. Tailored cybersecurity framework for educational institutions.

C. Implications for Policy and Practice

The implications of developing a tailored cybersecurity model are significant for policy and practice in educational institutions. First, this model can guide policymakers in developing regulations and policies that are more aligned with the needs of the education sector. For example, existing regulations may need to be adjusted to provide more flexibility to educational institutions in adopting relevant security controls without burdening them with unrealistic requirements.

Second, this model can assist educational institutions in managing cybersecurity risks more effectively and positively influence their performance, as shown in regional studies [36], without compromising core values like academic freedom and collaboration. By adopting a more modular and adaptable approach, educational institutions can notably enhance their cybersecurity stance while fostering an environment that promotes learning and innovation.

D. Comparison with Existing Studies

This research aligns with previous studies that have identified the shortcomings of current cybersecurity frameworks in meeting the specific needs of the education sector. For example, studies have shown that frameworks like NIST and ISO/IEC 27001 often fail to account for the decentralised nature and resource limitations typical of educational institutions [31],[33]. While these studies mainly examine the challenges of implementing existing frameworks, this research progresses the discussion by highlighting these weaknesses and proposing a customised cybersecurity model specifically designed for educational institutions, recognising the curriculum-level gaps still common in cybersecurity education [45].

Furthermore, existing literature emphasises adapting cybersecurity frameworks to fit the educational context better; however, it often stops short of providing actionable solutions [40], [37]. In contrast, this study offers practical guidance for developing and implementing a customised cybersecurity model, filling a critical literature gap. This research contributes significantly to the ongoing efforts to enhance cybersecurity in the education sector by addressing the challenges and providing concrete solutions.

E. Limitations and Future Research Directions

While this research provides valuable insights into the need for a tailored cybersecurity model in educational institutions, several limitations must be acknowledged. First, this research is limited to document analysis, so it does not include empirical data from implementing the proposed model. Therefore, further validation is needed through case studies or field experiments to test the effectiveness of this model in real-world contexts.

Additionally, this research focuses on educational institutions in countries with relatively advanced IT infrastructures. Future research should consider different contexts, such as academic institutions in developing countries, which may face various challenges in implementing cybersecurity.

Future research should also examine how new technologies, such as artificial intelligence (AI) and the Internet of Things (IoT), can be incorporated into a customised cybersecurity model and assist workforce development using established frameworks like NICE [38]. These technologies have significant potential to strengthen security, but also introduce new challenges that must be tackled.

VI. Conclusion and Recommendations

A. Summary of Key Findings

This research has conducted a comparative analysis of several cybersecurity frameworks used in educational institutions, including the NIST Cybersecurity Framework, ISO/IEC 27001, and COBIT. The main findings indicate that while these frameworks provide a solid foundation for cybersecurity management, they often do not fully align with educational institutions' unique needs. Implementation complexity, misalignment with academic culture, resource limitations, and decentralised organisational structures are the main challenges that hinder the practical application of existing frameworks in the education sector.

Based on the analysis results, this research proposes to develop a cybersecurity model explicitly tailored to the education sector. The proposed model emphasises flexibility, modularity, and resource optimisation, allowing educational institutions to adopt the most relevant security controls that align with their needs. This model supports the open and collaborative academic culture while maintaining high security standards.

B. Theoretical and Practical Contributions

This research makes significant contributions both theoretically and practically. Theoretically, it adds to the knowledge of the challenges and weaknesses of existing cybersecurity frameworks in the educational context. This research also offers an alternative model that is more suited to the needs of this sector, providing a foundation for further research to develop and test customised security models.

Practically, policymakers and practitioners in educational institutions can use the proposed model in this research to improve their cybersecurity posture. By adopting a more flexible and modular approach, educational institutions can more effectively manage cyber risks without compromising their core values, such as academic freedom and collaboration.

C. Limitations

While this research offers valuable insights, several limitations need to be acknowledged. This research is limited to document analysis and does not include empirical data from implementing the proposed model. Therefore, further research is required to test this model's effectiveness in real-world contexts. Additionally, this research focuses on educational institutions in countries with relatively advanced IT infrastructures so that different contexts may require adaptation of the proposed model.

D. Suggestions for Future Research

While this research provides valuable insights into the need for a customised cybersecurity model in educational institutions, further development is needed to address the sector's changing challenges. Future studies should aim to develop and empirically verify a cybersecurity framework specifically designed for educational settings. Such a framework should be adaptable and scalable, considering the diverse needs of institutions ranging from small K-12 schools to large universities. Research should investigate how this customised framework can incorporate emerging technologies like artificial intelligence (AI) and the Internet of Things (IoT) to strengthen cybersecurity without hindering academic freedom and collaboration. Additionally, the framework should be tested across different educational environments globally, including practical simulation settings like cyber ranges for training [48], to ensure its applicability and effectiveness in various cultural and organisational contexts.

Acknowledgment

This publication could not have been accomplished without the institution's extraordinary assistance. We also want to thank the reviewers whose suggestions will help tomake this manuscript eligible for publication.

References

[1] S. Saeed, "Digital transformation and cybersecurity challenges for businesses' resilience: issues and recommendations", Sensors, vol. 23, no. 15, p. 6666, 2023. https://doi.org/10.3390/s23156666

[2] J. Kumar, "Enhancing public awareness and education of ransomware attacks", 2023. https://doi.org/10.36227/techrxiv.24634806.v1

[3] S. S. Goswami, S. Sarkar, K. K. Gupta and S. Mondal "The role of cyber security in advancing sustainable digitalisation: opportunities and challenges", Journal of Decision Analytics and Intelligent Computing, vol. 3, no. 1, p. 270-285, 2023. https://doi.org/10.31181/jdaic10018122023g

[4] D. Hankerson, C. Venzke, E. Laird, H. Grant-Chapman, & D. Thakur, "Online and observed: student privacy implications of school-issued devices and student activity monitoring software", 2022. https://doi.org/10.31219/osf.io/73a2b

[5] H. Chou and C. Chou, "A multigroup analysis of factors underlying teachers' technostress and their continuance intention toward online teaching", Computers & Education, vol. 175, p. 104335, 2021. https://doi.org/10.1016/j.compedu.2021.104335

[6] K. Walker, K. Bodendorf, T. Kiesler, G. Mattos, M. Rostom, & A. Elkordy, "Compulsory technology adoption and adaptation in education: a looming student privacy problem", Journal of Consumer Affairs, vol. 57, no. 1, p. 445-478, 2023. https://doi.org/10.1111/joca.12506

[7] L. Yang, F. Martínez-Abad, & A. García-Holgado, "Exploring factors influencing pre-service and in-service teachers´ perception of digital competencies in the Chinese region of Anhui", Education and Information Technologies, vol. 27, no. 9, p. 12469-12494, 2022. https://doi.org/10.1007/s10639-022-11085-6

[8] S. Wang, "A review of research exploring pre-service teacher education for the digital era", International Journal of Education and Humanities, vol. 9, no. 1, p. 188-193, 2023. https://doi.org/10.54097/ijeh.v9i1.9407

[9] R. Chandarman and B. Niekerk, "Students' cybersecurity awareness at a private tertiary educational institution", The African Journal of Information and Communication, no. 20, 2017. https://doi.org/10.23962/10539/23572

[10] B. Blažič, "Cybersecurity skills in EU: new educational concept for closing the missing workforce gap", 2021. https://doi.org/10.5772/intechopen.97094

[11] R. Brink, J. Ophoff, & Z. Ruhwanya, "Relevant cybersecurity: curriculum guidance for the South African context", p. 3-19, 2022. https://doi.org/10.1007/978-3-031-21076-1_1

[12] R. Dontu, "An empirical paradigm on cybersecurity vulnerability mitigation framework", International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 9s, p. 786-792, 2023. https://doi.org/10.17762/ijritcc.v11i9s.9484

[13] N. Rahim, S. Hamid, M. Kiah, S. Shamshirband, & S. Furnell, "A systematic review of approaches to assessing cybersecurity awareness", Kybernetes, vol. 44, no. 4, p. 606-622, 2015. https://doi.org/10.1108/k-12-2014-0283

[14] Z. Ye, S. Liu, H. Zhang, & G. Wu, "Exploration and research on the training path of cybersecurity application-oriented talents by integrating industry and education", Education Journal, vol. 9, no. 5, p. 137, 2020. https://doi.org/10.11648/j.edu.20200905.13

[15] W. Triplett, "Addressing cybersecurity challenges in education", International Journal of Stem Education for Sustainability, vol. 3, no. 1, p. 47-67, 2023. https://doi.org/10.53889/ijses.v3i1.132

[16] M. Khader, M. Karam, & H. Fares, "Cybersecurity awareness framework for academia", Information, vol. 12, no. 10, p. 417, 2021. https://doi.org/10.3390/info12100417

[17] A. Alraddadi, "Developing an abstraction framework for managing and controlling Saudi banks' cybersecurity threats based on the NIST cybersecurity framework and iso/IEC 27001", Journal of Software Engineering and Applications, vol. 16, no. 12, p. 695-713, 2023. https://doi.org/10.4236/jsea.2023.1612036

[18] A. Adegbite, "Review of cybersecurity strategies in protecting national infrastructure: perspectives from the USA", Computer Science & IT Research Journal, vol. 4, no. 3, p. 200-219, 2023. https://doi.org/10.51594/csitrj.v4i3.658

[19] R. Pirta-Dreimane, A. Brilingaita, G. Majore, B. Knox, K. Lapin, K. Parish et al., "Application of intervention mapping in cybersecurity education design", Frontiers in Education, vol. 7, 2022. https://doi.org/10.3389/feduc.2022.998335

[20] Z. Ye, S. Liu, H. Zhang, & G. Wu, "Exploration and research on the training path of cybersecurity application-oriented talents by integrating industry and education", Education Journal, vol. 9, no. 5, p. 137, 2020. https://doi.org/10.11648/j.edu.20200905.13

[21] D. Onayemi, "Enhancing academic cybersecurity: integrated framework with network penetration testing", Social Science and Humanities Journal, vol. 7, no. 10, p. 3231-3245, 2023. https://doi.org/10.18535/sshj.v7i10.875

[22] B. Blažič, "Cybersecurity skills in EU: new educational concept for closing the missing workforce gap", 2021. https://doi.org/10.5772/intechopen.97094

[23] Sadiq Nasir "Exploring the effectiveness of cybersecurity training programs: factors, best practices, and future directions", Advances in Multidisciplinary & Scientific Research Journal Publication, vol. 2, no. 1, p. 151-160, 2023. https://doi.org/10.22624/aims/csean-smart2023p18

[24] W. Triplett, "Addressing cybersecurity challenges in education", International Journal of Stem Education for Sustainability, vol. 3, no. 1, p. 47-67, 2023. https://doi.org/10.53889/ijses.v3i1.132

[25] R. Pirta-Dreimane, A. Brilingaita, G. Majore, B. Knox, K. Lapin, K. Parish et al., "Application of intervention mapping in cybersecurity education design", Frontiers in Education, vol. 7, 2022. https://doi.org/10.3389/feduc.2022.998335

[26] S. Hakak, W. Khan, M. Imran, K. Choo, & M. Shoaib, "Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies", IEEE Access, vol. 8, p. 124134-124144, 2020. https://doi.org/10.1109/access.2020.3006172

[27] V. Agrawal, "A comparative study on information security risk analysis methods", Journal of Computers, p. 57-67, 2017. https://doi.org/10.17706/jcp.12.1.57-67

[28] R. Goel, A. Kumar, & J. Haddow, "Prism: a strategic decision framework for cybersecurity risk assessment", Information and Computer Security, vol. 28, no. 4, p. 591-625, 2020. https://doi.org/10.1108/ics-11-2018-0131

[29] A. Abohatem, "Suggestion cybersecurity framework (CSF) for reducing cyber-attacks on information systems", ل لعلوم صنعاء جامعة مجلة وال تكنولوجيا ال تطبيقية, vol. 1, no. 3, 2023. https://doi.org/10.59628/jast.v1i3.248

[30] T. Srivatanakul and F. Annansingh, "Incorporating active learning activities to the design and development of an undergraduate software and web security course", Journal of Computers in Education, vol. 9, no. 1, p. 25-50, 2021. https://doi.org/10.1007/s40692-021-00194-9

[31] A. Ghazvini, Z. Shukur, & Z. Hood, "Review of information security policy based on content coverage and online presentation in higher education", International Journal of Advanced Computer Science and Applications, vol. 9, no. 8, 2018. https://doi.org/10.14569/ijacsa.2018.090853

[32] Z. Ye, S. Liu, H. Zhang, & G. Wu, "Exploration and research on the training path of cybersecurity application-oriented talents by integrating industry and education", Education Journal, vol. 9, no. 5, p. 137, 2020. https://doi.org/10.11648/j.edu.20200905.13

[33] A. Dedeke and K. Masterson, "Contrasting cybersecurity implementation frameworks (CIF) from three countries", Information and Computer Security, vol. 27, no. 3, p. 373-392, 2019. https://doi.org/10.1108/ics-10-2018-0122

[34] A. Alraddadi, "Developing an abstraction framework for managing and controlling Saudi banks' cybersecurity threats based on the NIST cybersecurity framework and iso/IEC 27001", Journal of Software Engineering and Applications, vol. 16, no. 12, p. 695-713, 2023. https://doi.org/10.4236/jsea.2023.1612036

[35] M. Katsantonis and I. Mavridis, "Evaluation of hacklearn cofelet game user experience for cybersecurity education", International Journal of Serious Games, vol. 8, no. 3, p. 3-24, 2021. https://doi.org/10.17083/ijsg.v8i3.437

[36] B. M. Dioubate, W. D. W. Norhayate, Z. F. Anwar, S. Fauzilah .et. al. "The role of cybersecurity on the performance of Malaysian higher education institutions", Jurnal Pengurusan, vol. 67, 2023. https://doi.org/10.17576/pengurusan-2023-67-03

[37] R. Azmi, W. Tibben, & K. Win, "Review of cybersecurity frameworks: context and shared concepts", Journal of Cyber Policy, vol. 3, no. 2, p. 258-283, 2018. https://doi.org/10.1080/23738871.2018.1520271

[38] R. Petersen, D. Santos, M. Smith, & G. Witte, "Workforce framework for cybersecurity (nice framework)", 2020. https://doi.org/10.6028/nist.sp.800-181r1

[39] O. Folorunsho, A. Ayinde, M. A. Olagoke, O. E. Fatoye "Evaluating cybersecurity theories, models, standards and frameworks", Advances in Multidisciplinary & Scientific Research Journal Publication, vol. 5, no. 4, p. 61-66, 2019. https://doi.org/10.22624/aims/bhi/v5n4p7

[40] J. Hajný, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta, & R. Nicola, "Framework, tools and good practices for cybersecurity curricula", IEEE Access, vol. 9, p. 94723-94747, 2021. https://doi.org/10.1109/access.2021.3093952

[41] R. Pirta-Dreimane, A. Brilingaita, G. Majore, B. Knox, K. Lapin, K. Parish et al., "Application of intervention mapping in cybersecurity education design", Frontiers in Education, vol. 7, 2022. https://doi.org/10.3389/feduc.2022.998335

[42] M. Dawson, "Applying a holistic cybersecurity framework for global IT organisations", Business Information Review, vol. 35, no. 2, p. 60-67, 2018. https://doi.org/10.1177/0266382118773624

[43] K. Kioskli, T. Fotis, S. Nifakos, & H. Mouratidis, "The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0", Applied Sciences, vol. 13, no. 6, p. 3410, 2023. https://doi.org/10.3390/app13063410

[44] F. Salamah, "An adaptive cybersecurity training framework for the education of social media users at work", Applied Sciences, vol. 13, no. 17, p. 9595, 2023. https://doi.org/10.3390/app13179595

[45] I. Ngambeki, S. McBride, & J. Slay, "Knowledge gaps in curricular guidance for ics security", Journal of the Colloquium for Information Systems Security Education, vol. 9, no. 1, p. 6, 2022. https://doi.org/10.53735/cisse.v9i1.149

[46] M. Núñez, X. Palmer, L. Potter, C. Aliac, & L. Velasco, "ICT security tools and techniques among higher education institutions: a critical review", International Journal of Emerging Technologies in Learning (IJET), vol. 18, no. 15, p. 4-22, 2023. https://doi.org/10.3991/ijet.v18i15.40673

[47] N. Rahim, S. Hamid, M. Kiah, S. Shamshirband, & S. Furnell, "A systematic review of approaches to assessing cybersecurity awareness", Kybernetes, vol. 44, no. 4, p. 606-622, 2015. https://doi.org/10.1108/k-12-2014-0283

[48] S. Karagiannis, E. Magkos, E. Karavaras, A. Karnavas, M. Nikiforos, & C. Ntantogian, "Towards nice-by-design cybersecurity learning environments: a cyber range for SOC teams", 2022. https://doi.org/10.21203/rs.3.rs-1902186/v1

[49] G. Kabanda and T. Chingoriwo, "A cybersecurity culture framework for grassroots levels in Zimbabwe", Oriental Journal of Computer Science and Technology, vol. 14, no. 010203, p. 17-34, 2022. https://doi.org/10.13005/ojcst14.010203.03