Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

GenAI-Based Cybersecurity Adoption in Higher Education: A SWOT-Driven Responsible Implementation Framework

Pourya Nikfard

pourya.n@unimy.edu.my

University Malaysia of Computer Science and Engineering (UNIMY)

Anahita Ghanad

Veritas University College

Nursyakila Binti Abdul Aziz

Unitec Institute of Technology

Parham Nikfard

Loghman Hakim University

Perspective

Keywords: Generative Artificial Intelligence, cybersecurity, higher education, SWOT analysis, responsible AI, AI governance, cybersecurity adoption, organizational readiness

Posted Date: November 11th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11186493/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

GenAI-Based Cybersecurity Adoption in Higher Education: A SWOT-Driven Responsible Implementation Framework

Pourya Nikfard[1], Anahita Ghanad[2], Nursyakila Binti Abdul Aziz[3], Parham Nikfard[4]

[1] School of Computing and Digital Technology, University Malaysia of Computer Science and Engineering (UNIMY), Selangor, Malaysia
[2] School of Education, Veritas University College, Selangor, Malaysia
[3] School of Business, Unitec, Te Pūkenga, Auckland, New Zealand
[4] School of Technology and Civil, Loghman Hakim University, Gorgan, Iran

Abstract

The rapid digital transformation of higher education has increased dependence on cloud platforms, learning management systems, online assessment systems, research repositories, enterprise applications, and interconnected digital services. At the same time, this transformation has also considerably increased cyber risks facing higher education institutions (HEIs). Generative Artificial Intelligence (GenAI) enables threat-intelligence analysis, security-log interpretation, anomaly investigation, incident-response assistance, and cybersecurity knowledge management. However, adoption brings challenges involving hallucination, privacy, organizational readiness, human oversight, accountability, regulatory compliance, and adversarial misuse. Existing cybersecurity and AI governance frameworks serve as foundational guidance, although they primarily concern cybersecurity risk management or AI governance independently and do not provide a holistic adoption framework explicitly focused on GenAI-based cybersecurity for HEI infrastructure. This paper presents a SWOT-based responsible adoption model composed of five aspects: GenAI cybersecurity capabilities, organizational readiness, ethical governance, regulatory compliance, and cybersecurity outcomes. A single comparative document analysis assesses the proposed framework with the NIST Cybersecurity Framework (CSF) 2.0, NIST Artificial Intelligence Risk Management Framework (AI RMF) with its Generative AI Profile, ISO/IEC 42001, and higher-education cybersecurity guidance. This decision model utilizes nine evaluation criteria to review cybersecurity capability, GenAI specificity, organizational readiness, ethical governance, regulatory alignment, human oversight, higher-education contextualization, measurable cybersecurity outcomes, and implementation decision support. Results suggest that established frameworks offer robust but varying emphases of coverage, while the proposed model consolidates these concerns into an HEI-specific adoption decision layer. The framework aims to guide HEIs not only in understanding how GenAI can assist with cybersecurity, but also in determining whether the institution is prepared to apply it responsibly, what governance mechanisms should be established, and how its value can be evaluated.

Keywords— Generative Artificial Intelligence, cybersecurity, higher education, SWOT analysis, responsible AI, AI governance, cybersecurity adoption, organizational readiness

I. Introduction

Digital transformation is now at the core of modern higher education. Universities are increasingly reliant on learning management systems, cloud computing, student information systems, digital assessment platforms, research repositories, enterprise applications, online collaboration services, and interconnected information infrastructures. These technologies enhance access, operational efficiency, teaching quality, research collaboration, and institutional management. However, they also increase the number of applications, users, devices, interfaces, databases, and data repositories that need to be secured. Higher education institutions represent particularly complex cybersecurity environments. Unlike highly centralized commercial organizations, universities must simultaneously enable academic freedom, openness, research collaboration, student access, external partnerships, and distributed decision-making. University environments house sensitive student and employee information, financial records, research data, intellectual property, authentication credentials, examination information, and confidential institutional documents. Thus, cybersecurity in higher education requires a balance between protection and openness. EDUCAUSE and the Higher Education Information Security

[1] Correspondent author: pourya_nikfard@yahoo.com

Council have highlighted the need for higher education to embrace context-aware cybersecurity practices rather than relying on a one-size-fits-all approach (EDUCAUSE Higher Education Information Security Council [HEISC], n.d.; Cummings & Grama, 2016).

GenAI adds a new layer of opportunity and risk. Large language models and related generative systems can summarize threat intelligence, analyze logs, help investigate incidents, find security knowledge, create documentation, and assist analysts. However, LLMs also pose risks such as hallucination, prompt injection, data leakage, insecure outputs, over-reliance, and adversarial misuse (Curran et al., 2024; Uddin et al., 2025; Zhang et al., 2025). Hence, the question considered in this paper is not just whether GenAI can advance cybersecurity. This turns into an institutional question: How can an institution of higher learning decide, if at all, whether GenAI is suitable for use in cybersecurity on its own campus? Different existing standards and frameworks, such as the NIST CSF 2.0, NIST AI RMF, its Generative AI Profile, and ISO/IEC 42001, provide valuable guidance (Autio et al., 2024; International Organization for Standardization [ISO], 2023; Pascoe et al., 2024; Tabassi, 2023). However, none of these is specifically designed as an HEI-focused adoption model that combines strategic SWOT analysis, cybersecurity capabilities, institutional readiness, responsible governance, regulatory alignment, and measurable cybersecurity outcomes.

This paper has four contributions. First, it develops a five-dimensional responsible GenAI cybersecurity adoption model for HEIs. Second, instead of using SWOT merely as a descriptive technique, it conceptualizes SWOT as the strategic layer of adoption. Third, it conducts a comparative document analysis with well-established cybersecurity and AI governance instruments. Fourth, it elaborates on why the proposed framework can complement current standards by serving as an HEI-specific decision and implementation layer.

II. Related Work

A. GenAI and Cybersecurity

GenAI and LLMs have been increasingly explored across cybersecurity tasks such as threat intelligence, security question answering, vulnerability analysis, malware analysis, phishing analysis, incident response, security operations, and cybersecurity education (Curran et al., 2024; Uddin et al., 2025; Zhang et al., 2025). Survey overviews on the topic report that LLMs may decrease analyst effort and make cybersecurity knowledge more accessible, while trustworthiness, hallucination, security of the models themselves, privacy, and evaluation remain relevant issues.

B. Cybersecurity in Higher Education

HEIs have unique cybersecurity challenges because they combine massive and diverse user bases with relatively decentralized management, research openness, legacy systems, cloud services, and confidential data. Recent studies on AI-based and traditional approaches to cybersecurity in online higher education suggest that organizations need strategies that balance technical cybersecurity controls with organizational and educational concerns (Parambil et al., 2024). Collaborative higher-education cybersecurity research also focuses on incident response, knowledge sharing, awareness, and coordination (Otoom et al., 2025).

The organizational dimension of cybersecurity adoption is also consistent with earlier research on enterprise architecture implementation. Enterprise architecture implementation requires alignment between organizational objectives and information technology, while implementation methodologies must account for practices, organizational factors, governance, requirements, and continual improvement (Rouhani et al., 2013, 2015a, 2015b, 2015c). Comparative research has further demonstrated that different implementation methodologies possess different strengths and limitations and therefore should be selected according to organizational requirements and implementation contexts (Rouhani et al., 2013). These findings are relevant to GenAI cybersecurity adoption because the introduction of GenAI into an HEI similarly requires alignment between technological capability, institutional objectives, organizational readiness, governance, and implementation conditions.

C. NIST Cybersecurity Framework 2.0

The NIST CSF 2.0 offers a scalable and customizable model for organizations to understand, assess, prioritize, and communicate cybersecurity risk. Its six functions are Govern, Identify, Protect, Detect, Respond, and Recover (Pascoe et al., 2024). While useful for an institutional cybersecurity strategy, the framework is intentionally sector-agnostic and does not constitute a GenAI-specific adoption decision model for HEIs.

D. NIST AI RMF and Generative AI Profile

The NIST AI RMF offers guidance at a high level to support the integration of trustworthiness considerations in the design, development, use, and evaluation of AI systems (Tabassi, 2023). The Generative AI Profile builds upon this strategy by addressing risks specific to generative AI and is designed to assist organizations in recognizing and managing these risks across the AI lifecycle (Autio et al., 2024).

E. ISO/IEC 42001

The requirements of ISO/IEC 42001 for an Artificial Intelligence Management System enable organizations to develop, establish, implement, maintain, and continuously improve AI governance (ISO, 2023). It therefore offers an organizational management-system viewpoint, but does not explicitly prescribe which GenAI cybersecurity features an HEI should focus on or how SWOT elements should affect selection.

F. Higher-Education Governance and Workforce

HEI cybersecurity is also dependent on governance, workforce capability, and institutional coordination. EDUCAUSE regards governance as a mechanism for bringing cybersecurity goals and institutional missions into alignment (Parker et al., 2024). The NIST NICE Workforce Framework provides a unified construct for cybersecurity work, knowledge, skills, tasks, and roles (Petersen et al., 2020).

Organizational capability and implementation effectiveness are not determined solely by the availability of technology. Previous research on enterprise architecture implementation identified alignment, adaptiveness, support, binding, and innovation as factors associated with implementation effectiveness (Rouhani et al., 2015c). Other work emphasized governance, requirements analysis, evaluation, implementation guidance, and continual improvement as important elements of implementation methodology (Rouhani et al., 2015a, 2015b). These observations support the present framework's emphasis on organizational readiness and governance as essential conditions for responsible GenAI cybersecurity adoption.

G. Software Testing, Evaluation, and Measurable Outcomes

Evaluation and measurable outcomes are also important in software engineering research. Previous studies by Nikfard and colleagues investigated model testability through empirical studies, comparative evaluation, and assessment of testability approaches (Nikfard et al., 2013a, 2013b, 2013c). This research emphasized the importance of evaluating software artifacts and testing characteristics systematically rather than assuming that a technically developed system is automatically effective. Related work on web application testing examined functional testing and comparative evaluation of testing approaches (Nikfard & Selamat, 2012; Nikfard et al., 2013d).

These principles are relevant to GenAI cybersecurity because adoption should similarly be evaluated through explicit operational indicators rather than through technological capability alone. Software evolution also demonstrates the importance of understanding relationships among changing requirements, software artifacts, and impact analysis (Abolghasem Zadeh et al., 2013). In a GenAI cybersecurity environment, changes to models, prompts, data sources, security policies, or organizational requirements may similarly affect multiple institutional artifacts and controls. Consequently, continuous evaluation and change management should form part of responsible adoption.

H. Research Gap

The literature confirms that cybersecurity, AI risk management, AI governance, higher-education cybersecurity, and workforce development are areas in which established sources exist. The relatively unexplored gap is the synthesis of these areas into a model of adoption specifically for GenAI-based cybersecurity in HEIs. It is this integration that the proposed framework addresses.

III. Research Methodology

A. Research Design

This study adopts a comparative document analysis approach. The objective is to evaluate whether the proposed framework offers an integrated set of dimensions relevant to responsible GenAI cybersecurity adoption in HEIs. The paper does not claim stakeholder-interview validation, but rather a structured framework-level evaluation that can subsequently be followed by empirical validation.

B. Frameworks Selected

Four reference cases were selected: the NIST CSF 2.0, NIST AI RMF and its Generative AI Profile, ISO/IEC 42001, and higher-education cybersecurity resources from EDUCAUSE and HEISC.

C. Evaluation Criteria

Each criterion is coded as 1 when explicitly integrated and 0 when not explicitly integrated as a central element. Broad relevance is not treated as equivalent to explicit integration.

Table 1: Evaluation Criteria for Comparative Framework Analysis

Code	Criterion	Operational definition
C1	Cybersecurity capability	Explicit support for cybersecurity operational capabilities
C2	GenAI specificity	Explicit attention to generative AI
C3	Organizational readiness	Leadership, skills, infrastructure, resources, and culture
C4	Ethical governance	Privacy, transparency, accountability, and responsible use
C5	Regulatory alignment	Legal, regulatory, policy, and compliance considerations
C6	Human oversight	Human review and accountability
C7	HEI contextualization	Explicit higher-education context
C8	Cybersecurity outcomes	Measurable cybersecurity performance/outcomes
C9	Implementation decision support	Support for deciding whether/how to adopt GenAI

D. Comparative Dataset

The analysis is based on five frameworks/resources and nine criteria, resulting in 45 framework-criterion observations. The matrix is an author-designed comparison, not an externally validated scoring instrument. Future studies should incorporate multiple coders and inter-rater reliability.

IV. Proposed SWOT-Driven Responsible Implementation Framework

The framework has five interconnected dimensions: (1) GenAI cybersecurity capabilities, (2) organizational readiness, (3) ethical governance, (4) regulatory alignment, and (5) cybersecurity outcomes. SWOT is a strategic assessment layer that spans the five dimensions.

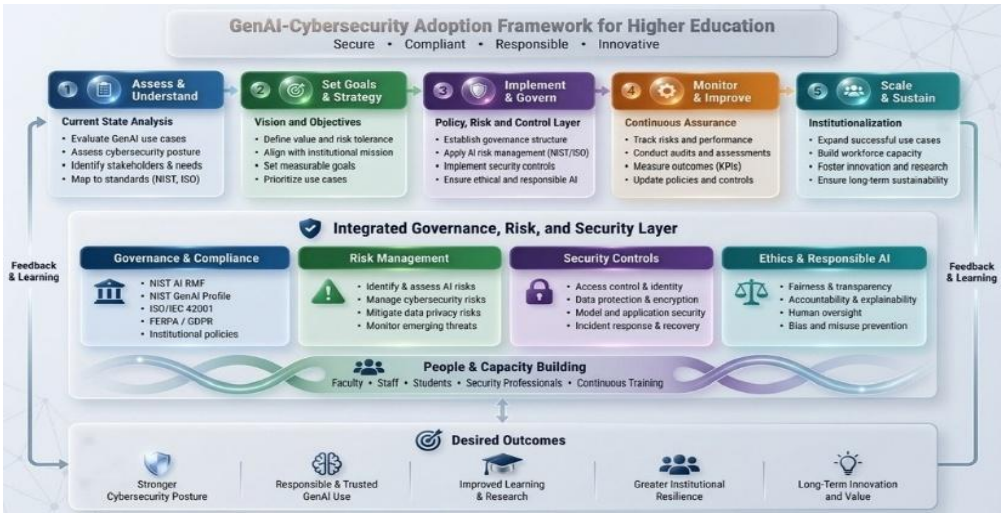


Figure 1. Proposed GenAI-Based Cybersecurity Adoption Framework

A. GenAI Cybersecurity Capabilities

The first facet identifies specific cybersecurity challenges for which GenAI could be relevant. Possible uses include threat-intelligence analysis, security-log summarization, anomaly explanation, incident analysis, vulnerability analysis, security knowledge management, incident-response assistance, and analyst decision support.

B. Organizational Readiness

Organizational readiness is the organizational capacity to adopt, operate, monitor, customize, and maintain GenAI. Critical elements consist of leadership, cybersecurity maturity, AI expertise, workforce capability, workforce training, budget, infrastructure, data governance, culture, and integration capability.

C. Ethical Governance

Ethical governance involves privacy, transparency, explainability, fairness, accountability, human oversight, and responsible data stewardship. As GenAI outputs may be false or context-inappropriate, significant decisions with respect to cybersecurity should still be reviewed by humans. AI governance research similarly emphasizes the need to address organizational, ethical, and accountability dimensions rather than treating AI governance as a purely technical issue (Batool et al., 2025).

D. Regulatory Alignment

HEIs are subject to data-protection, cybersecurity, research-ethics, institutional-policy, contractual, and emerging AI governance obligations. Hence, regulatory harmonization is conceived as a continuous evaluation.

E. Cybersecurity Outcomes

The framework calls for quantifiable evidence of benefits. Possible metrics include detection performance, time to respond to an incident, analyst workload, time spent investigating, efficiency of alert triage, false-positive rates, severity of incidents, user acceptance, privacy incidents, and compliance performance.

The emphasis on measurable outcomes is consistent with previous research on model testability and software testing (Nikfard et al., 2013a, 2013b, 2013c, 2013d). Testability research has highlighted the importance of assessing whether software artifacts can be effectively validated and tested, while comparative testing research has examined differences among alternative testing approaches. The proposed GenAI cybersecurity framework extends this evaluation principle from individual software artifacts to institutional cybersecurity adoption by requiring measurable evidence of operational value. Accordingly, detection performance, response time, analyst workload, false-positive rates, alert-triage efficiency, and other indicators should be established before and after implementation.

V. Data Analysis and Results

A. Comparative Coverage Matrix

The matrix shows that the proposed framework explicitly integrates all nine criteria. The result should be interpreted as structural alignment with the evaluation criteria, not proof that the proposed framework is universally superior. Each reference framework was developed for a different purpose.

Table 2: Comparative Coverage of GenAI Cybersecurity Adoption Criteria Across Frameworks

Criterion	**NIST CSF 2.0**	**NIST AI RMF/GAI**	**ISO/IEC 42001**	**HEI guidance**	**Proposed**
C1 Cybersecurity capability	1	0	0	1	1
C2 GenAI specificity	0	1	0	0	1
C3 Organizational readiness	1	1	1	1	1
C4 Ethical governance	0	1	1	1	1
C5 Regulatory alignment	1	1	1	1	1
C6 Human oversight	0	1	1	1	1
C7 HEI contextualization	0	0	0	1	1
C8 Cybersecurity outcomes	1	0	0	1	1
C9 Implementation decision support	0	0	0	0	1
Coverage	**4/9**	**5/9**	**4/9**	**6/9**	**9/9**
Percentage	**44.4%**	**55.6%**	**44.4%**	**66.7%**	**100%**

B. Interpretation of Results

NIST CSF 2.0 provides robust cybersecurity capability, organizational, regulatory, and outcome-oriented coverage (Pascoe et al., 2024). NIST AI RMF and the Generative AI Profile have a stronger focus on AI and GenAI risk, including trustworthiness and human-centered considerations (Autio et al., 2024; Tabassi, 2023). ISO/IEC 42001 offers an organizational management-system approach to AI governance (ISO, 2023). Higher-education guidance adds sector-specific considerations, governance, and institutional context (EDUCAUSE HEISC, n.d.; Parker et al., 2024). The proposed framework integrates these aspects and explicitly adds an adoption decision layer and a SWOT mechanism.

C. Comparative Strength of the Proposed Framework

The primary finding is not that current frameworks are insufficient. Instead, the analysis shows a complementary relationship. Current frameworks help answer important questions about cybersecurity risk, AI risk, and AI governance. The proposed framework helps answer the organizational question: Should an HEI use GenAI to solve a certain cybersecurity problem, and what needs to be in place for the solution to be implemented and maintained?

VI. Framework Evaluation and Contribution

A. Integration Rather Than Replacement

The framework should be implemented as an integration layer. NIST CSF can help with cybersecurity controls and outcomes; NIST AI RMF and its Generative AI Profile can help with AI and GenAI risk management;

ISO/IEC 42001 can help with institutional AI governance; and higher-education guidance can provide institutional context (Autio et al., 2024; ISO, 2023; Pascoe et al., 2024; Tabassi, 2023).

B. Higher-Education-Specific Context

Universities have to find a balance between cybersecurity and academic freedom, open research, student access, decentralized governance, research confidentiality, and resource constraints. The framework explicitly incorporates these elements into organizational readiness, SWOT, governance, and outcomes.

The organizational emphasis of the proposed framework is also supported by enterprise architecture research. A systematic literature review of enterprise architecture implementation methodologies identified implementation practices, organizational factors, tools, and unresolved implementation problems as important considerations for effective implementation (Rouhani et al., 2015a). Comparative studies of implementation methodologies further demonstrate that organizations need to consider differences among methodologies rather than assume that one implementation approach is universally appropriate (Rouhani et al., 2013). Research into critical success factors and implementation effectiveness similarly emphasizes organizational alignment, adaptability, support, governance, and innovation (Nikpay et al., 2013; Rouhani et al., 2015c). These findings reinforce the proposition that GenAI cybersecurity adoption in HEIs should be treated as an organizational and socio-technical transformation rather than simply as the deployment of an AI technology.

C. SWOT as a Decision Layer

SWOT is an operational decision mechanism. Strengths are the abilities that can be used; weaknesses are internal limitations; opportunities are institutional value; and threats are the risks that need to be mitigated.

D. Outcome-Oriented Adoption

The framework does not assume that implementation itself constitutes success. The GenAI cybersecurity system should demonstrate measurable improvement. The institution should either change, limit, or stop implementing the technology if it does not enhance security performance or poses unacceptable risks.

The outcome-oriented principle also builds upon previous work in software testing and evaluation. Research on model testability has examined systematic approaches for evaluating testability and comparing alternative testability models (Nikfard et al., 2013a, 2013b, 2013c), while research on web application testing has considered functional testing and comparative testing approaches (Nikfard & Selamat, 2012; Nikfard et al., 2013d). These studies provide methodological support for the principle that technology adoption should be accompanied by explicit evaluation criteria and measurable outcomes.

E. Responsible Adoption

Responsible adoption is defined in the framework as the interplay between cybersecurity effectiveness, organizational readiness, ethical governance, regulatory alignment, and continuous outcome evaluation.

VII. Why HEIs Should Use the Proposed Framework

The framework offers a tangible pre-adoption and continuous-evaluation mechanism. It can be employed prior to procurement, throughout pilot implementation, and periodically in governance reviews. The proposed staged adoption process is also consistent with earlier research on implementation methodologies, where successful implementation requires structured planning, alignment, requirements analysis, governance, evaluation, and continual improvement (Nikpay et al., 2013; Rouhani et al., 2013, 2015a, 2015b, 2015c). In this study, these implementation principles are adapted to the specific challenges of GenAI-based cybersecurity in HEIs.

Table 3: Proposed Institutional GenAI Cybersecurity Adoption Process

Stage	Action
1. Identify the cybersecurity problem	Define the operational problem, such as alert overload, slow investigation, threat-intelligence gaps, or analyst workload.
2. Evaluate GenAI capability	Determine whether GenAI provides a genuine advantage for the identified problem.
3. Conduct SWOT analysis	Assess internal strengths and weaknesses and external opportunities and threats.
4. Assess organizational readiness	Evaluate leadership, skills, infrastructure, resources, data, and integration.
5. Apply ethical governance	Define privacy, human oversight, transparency, accountability, and data-management controls.
6. Conduct regulatory assessment	Identify applicable laws, institutional policies, contracts, and research requirements.
7. Implement a controlled pilot	Start with a relatively low-risk cybersecurity use case.
8. Measure outcomes	Evaluate predefined technical, operational, and governance indicators.
9. Decide whether to scale	Scale, modify, restrict, or suspend according to evidence.

VIII. Institutional Adoption Assessment Model

The framework can be operationalized through a five-point institutional assessment. Scores range from 1 (very low readiness) to 5 (very high readiness).

Table 4: Institutional GenAI Cybersecurity Adoption Readiness Scale

Score	Interpretation	Suggested action
1	Very low	Do not deploy; address critical gaps
2	Low	Preparation required
3	Moderate	Controlled pilot
4	High	Controlled implementation
5	Very high	Suitable for broader deployment

An illustrative Adoption Readiness Score (ARS) can be calculated as:

$$\mathbf{ARS = (\Sigma Si / 5n) \times 100}$$

where Si is the score for indicator i and n is the number of indicators. The score is a proposed research instrument; thresholds require empirical validation.

Table 5: Dimensions and Example Indicators for Adoption Readiness Assessment

Dimension	Example indicators
GenAI capability	Threat analysis, log interpretation, response support

Organizational readiness	Skills, leadership, infrastructure, budget, integration
Ethical governance	Privacy, explainability, human oversight, accountability
Regulatory alignment	Data protection, institutional policy, research ethics
Cybersecurity outcomes	Detection, response time, workload, resilience

IX. Discussion

These results support the position that prudent GenAI cybersecurity investment is more of a socio-technical issue than a purely technological one. The comparison shows that existing models serve different and complementary purposes. The proposed framework addresses a pragmatic limitation of technology-focused adoption models: they may emphasize the question of whether a technology is ready without sufficient emphasis on whether the organization is ready to determine whether the use of the technology is safe and whether adoption will produce quantifiable value.

The proposed model makes an explicit connection between capability and readiness, governance, regulation, and outcomes. Such an approach is critical to HEIs in particular, since cybersecurity decisions can impact many varied individuals. An automated recommendation that might be acceptable in a low-impact environment could be inappropriate if it disables a student account, halts a research environment, leaks sensitive research data, or triggers a major infrastructural overhaul. The proposed framework therefore enables step-by-step realization. Lower-risk activities such as threat-report summarization, security knowledge retrieval, and analyst write-up can be deployed prior to the introduction of higher-risk decision-support and semi-automated response activities.

The findings are also consistent with the broader software engineering literature on implementation and evaluation. Enterprise architecture research has shown that implementation effectiveness depends on organizational and methodological factors rather than technology alone (Nikpay et al., 2013; Rouhani et al., 2015a, 2015c). Similarly, research on software testing and model testability emphasizes the importance of systematic evaluation and measurable characteristics (Nikfard et al., 2013a, 2013b, 2013c, 2013d). The proposed framework brings these principles together in the GenAI cybersecurity domain by linking technological capability with organizational readiness, governance, regulatory requirements, and measurable cybersecurity outcomes.

X. Practical and Research Implications

The proposed framework has practical and research implications for higher education institutions by supporting collaboration among university leaders, CIOs, CISOs, IT and cybersecurity teams, academic management, data-protection officers, legal and compliance units, and researchers in the responsible adoption of GenAI for cybersecurity. For cybersecurity practitioners, the framework provides a structured basis for prioritizing GenAI applications, assessing cybersecurity capabilities, and determining appropriate levels of human oversight. From a policy perspective, it can support the development of institutional AI and cybersecurity policies by providing a common operating picture that integrates technical capability, organizational readiness, ethical governance, regulatory alignment, and cybersecurity outcomes. From a research perspective, the framework introduces measurable dimensions that can be empirically evaluated, enabling future studies to investigate the relationships among institutional readiness, GenAI capability, governance, regulatory compliance, human oversight, and cybersecurity performance.

XI. Conclusion

GenAI could be highly beneficial in addressing cybersecurity challenges in higher education, but having the technical means does not ensure that adoption will be effective or responsible. Universities have to address cybersecurity needs on the one hand and organizational readiness on the other, while also dealing with ethical governance, regulatory compliance, and tangible results. This paper presents a responsible implementation framework for GenAI informed by SWOT analysis and composed of five interrelated layers: GenAI cybersecurity capabilities, ethical governance, organizational readiness, regulatory alignment, and cybersecurity outcomes.

Comparative document analysis highlights that useful but diverse perspectives can be found in existing cybersecurity, AI governance, and higher-education documentation. In doing so, the paper contributes an HEI-specific adoption and decision layer that is cognizant of these concerns.

The main value of this framework lies in its shift in the institutional adoption question. An HEI should ask not only whether GenAI can be used to improve cybersecurity, but whether the institution is ready to employ GenAI for a specific cybersecurity issue, whether the deployment can be governed responsibly, whether regulatory conditions support the decision, and whether it is possible to demonstrate quantifiable improvements in cybersecurity.

The framework should be viewed as reinforcing established standards rather than replacing them. Its next step should be to validate it empirically with HEI stakeholders and real-life implementation data.

XII. Limitations and Future Research

There are three main limitations of this study. First, the framework evaluation is based on document analysis, not stakeholder interviews or real-world deployment. Second, the binary coding scheme oversimplifies complex frameworks and may miss some details. Third, the evaluation criteria were tailored to the research problem and have not yet been independently validated.

Future research should employ multiple independent coders and calculate inter-rater reliability. Empirical validation should involve university cybersecurity professionals, IT managers, AI governance personnel, data-protection officers, academic leaders, and technology decision-makers. A mixed-method study could combine semi-structured interviews with a questionnaire and real-world pilot measurements. A follow-up study could potentially explore the framework in a number of HEIs and test for a correlation between higher Adoption Readiness Scores and better implementation outcomes.

Declarations

Funding Declaration

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Clinical Trial Number

Clinical trial number: not applicable.

Ethics, Consent to Participate and Consent to Publish

Ethics, Consent to Participate and Consent to Publish declarations: not applicable.

References

Abolghasem Zadeh, M. H., Kama, M. N., Nikfard, P., & Ibrahim, S. B. (2013). Software changes: Related software artifacts and their relationships. In *The second international conference on advances in computing and networking*. https://doi.org/10.3850/978-981-07-5939-1_01

Autio, C., Schwartz, R., Dunietz, J., Jain, S., Stanley, M., Tabassi, E., Hall, P., & Roberts, K. (2024). *Artificial intelligence risk management framework: Generative artificial intelligence profile* (NIST AI 600-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.600-1

Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: A systematic literature review. *AI and Ethics, 5*, 3265–3279. https://doi.org/10.1007/s43681-024-00653-w

Bittle, K., & El-Gayar, O. (2025). Generative AI and academic integrity in higher education: A systematic review and research agenda. *Information, 16*(4), 296.

Cummings, J., & Grama, J. (2016). *EDUCAUSE comments: NIST critical infrastructure cybersecurity framework*. EDUCAUSE.

Curran, K., Curran, E., Killen, J., & Duffy, C. (2024). The role of generative AI in cybersecurity. *MET Journal, 5*(2).

EDUCAUSE Higher Education Information Security Council. (n.d.). *Information security guide: Effective practices and solutions for higher education*. EDUCAUSE.

International Organization for Standardization. (2023). *ISO/IEC 42001:2023 information technology—Artificial intelligence—Management system*. ISO.

Mak, J., Nakatumba-Nabende, J., Clear, A., et al. (2025). Navigating the ethical and societal impacts of generative AI in higher computing education. *arXiv*.

Najaftorkaman, M., Nikfard, P., Masrom, M., & Abbasy, M. (2011). An efficient cryptographic protocol based on DNA chip. *Procedia Engineering*.

Nikfard, P., & Selamat, H. (2012). Functional testing on web applications. In *Postgraduate annual research on informatics seminar (PARIS 2012)*.

Nikfard, P., Ibrahim, S. B., Rohani, B. D., Selamat, H. B., & Mahrin, M. N. (2013a). A comparative evaluation of approaches for model testability. *International Journal of Computers & Technology, 9*(1), 948–955. https://doi.org/10.24297/ijct.v9i1.4157

Nikfard, P., Ibrahim, S. B., Rohani, B. D., Selamat, H. B., & Mahrin, M. N. (2013b). An evaluation for model testability approaches. *International Journal of Computers & Technology, 9*(1), 938–947. https://doi.org/10.24297/ijct.v9i1.4159

Nikfard, P., Najafabadi, M. K., Rouhani, B. D., Nikpay, F., & Selamat, H. B. (2013c). An empirical study into model testability. In *2013 International Conference on Informatics and Creative Multimedia* (pp. 85–92). IEEE. https://doi.org/10.1109/ICICM.2013.22

Nikfard, P., Abolghasem Zadeh, M. H., & Ibrahim, S. B. (2013d). A comparative evaluation of approaches for web application testing. In *International Conference on Soft Computing and Software Engineering*.

Nikpay, F., Selamat, H., Rouhani, B. D., & Nikfard, P. (2013). A review of critical success factors of enterprise architecture implementation. In *2013 International Conference on Informatics and Creative Multimedia* (pp. 38–42). IEEE.

Nott, C. (2025). Organizational adaptation to generative AI in cybersecurity: A systematic review. *arXiv:2506.12060*.

Otoom, A. A., Atoum, I., Al-Harahsheh, H., Aljawarneh, M., Al Refai, M. N., & Baklizi, M. (2025). A collaborative cybersecurity framework for higher education. *Information and Computer Security, 33*(3), 362–389. https://doi.org/10.1108/ICS-02-2024-0048

Parambil, M. M. A., Rustamov, J., Ahmed, S. G., Rustamov, Z., Awad, A. I., Zaki, N., & Alnajjar, F. (2024). Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. *Computers and Education: Artificial Intelligence, 7*, 100327. https://doi.org/10.1016/j.caeai.2024.100327

Parker, M., Jackson, D., Porter, A., Hoffman, J., Tylutki, J., & Arbino, N. (2024). *Cybersecurity governance toolkit*. EDUCAUSE Review.

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). National Institute of Standards and Technology.

Petersen, R., Santos, D., Wetzel, K., Smith, M., & Witte, G. (2020). *Workforce framework for cybersecurity (NICE framework)* (NIST SP 800-181 Rev. 1). National Institute of Standards and Technology.

Qadhi, S. M., Alduais, A., Chaaban, Y., & Khraisheh, M. (2024). Generative AI, research ethics, and higher education: Scientometric insights. *Information, 15*(6), 325.

Rouhani, B. D., Mahrin, M. N., Nikpay, F., & Nikfard, P. (2013). A comparison of enterprise architecture implementation methodologies. In *2013 International Conference on Informatics and Creative Multimedia* (pp. 1–6). IEEE. https://doi.org/10.1109/ICICM.2013.9

Rouhani, B. D., Mahrin, M. N., Nikpay, F., & Nikfard, P. (2015a). A systematic literature review on enterprise architecture implementation methodologies. *Information and Software Technology, 62*, 1–20. https://doi.org/10.1016/j.infsof.2015.01.012

Rouhani, B. D., Mahrin, M. N., Nikpay, F., Nikfard, P., & Najafabadi, M. K. (2015b). Factors that affect the effectiveness of enterprise architecture implementation methodology. *International Journal of Economics and Management Engineering, 9*(1), 19–25.

Rouhani, B. D., Mahrin, M. N., Nikpay, F., Nikfard, P., & Darvish Rouhani, B. (2015c). Agent-oriented based enterprise architecture implementation methodology. In *New contributions in information systems and technologies* (Advances in Intelligent Systems and Computing, Vol. 353, pp. 411–419). Springer. https://doi.org/10.1007/978-3-319-16486-1_41

Rouhani, B. D., Mahrin, M. N., Nikfard, P., & Nikpay, F. (2014). The role of agent-oriented technology on developing an enterprise architecture implementation methodology. In *2014 8th Malaysian Software Engineering Conference (MySEC)* (pp. 331–335). IEEE. https://doi.org/10.1109/MySec.2014.6986039

Tabassi, E. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). National Institute of Standards and Technology.

Taeihagh, A. (2025). Governance of generative AI. *Policy and Society, 44*(1), 1–22.

Tian, J. (2025). Integrating artificial intelligence into the cybersecurity curriculum in higher education: A systematic literature review. *Education Sciences, 15*(11), 1540. https://doi.org/10.3390/educsci15111540

Uddin, M., Irshad, M. S., Kandhro, I. A., et al. (2025). Generative AI revolution in cybersecurity: A comprehensive review of threat intelligence and operations. *Artificial Intelligence Review, 58*, 236. https://doi.org/10.1007/s10462-025-11219-5

Yusuf, Y., Pervin, N., & Román-González, M. (2024). Generative AI and the future of higher education: A threat to academic integrity or reformation? Evidence from multicultural perspectives. *International Journal of Educational Technology in Higher Education, 21*, 21.

Zhang, J., Bu, H., Wen, H., Liu, Y., Fei, H., Xi, R., Li, L., Yang, Y., Zhu, H., et al. (2025). When LLMs meet cybersecurity: A systematic literature review. *Cybersecurity, 8*, 55. https://doi.org/10.1186/s42400-025-00361-w

Abbasy, M. R., Nikfard, P., Ordi, A., & Torkaman, M. R. N. (2012). DNA base data hiding algorithm. *International Journal of New Computer Architectures and their Applications, 2*(1), 183–192.

Najaf Torkaman, M. R., Nikfard, P., Kazazi, N. S., Abbasy, M. R., & Tabatabaiee, S. F. (2011). Improving hybrid cryptosystems with DNA steganography. In *Digital enterprise and information systems* (Communications in Computer and Information Science, Vol. 194, pp. 42–52). Springer.

Parker, M., Jackson, D., Porter, A., Hoffman, J., Tylutki, J., & Arbino, N. (2024). *Cybersecurity governance toolkit*. EDUCAUSE Review.