

Article

Building Safe and Sustainable Universities: An Integrated Governance Framework for Physical, Cyber, and Psychosocial Security

Miroslav Betuš ^{1,*} , Ivanna Betušová ¹ , Gabriel Wittenberger ¹ , Martin Konček ¹  and Marek Hnilica ² 

¹ Faculty of Mining, Process Control and Geotechnologies, Technical University of Košice, 04001 Košice, Slovakia; ivanna.betusova@tuke.sk (I.B.); gabriel.wittenberger@tuke.sk (G.W.); martin.koncek@tuke.sk (M.K.)

² Faculty of Logistics and Crisis Management, Tomas Bata University in Zlín, Studentské nám. 1532, 68601 Uherské Hradiště, Czech Republic; hnilica@utb.cz

* Correspondence: miroslav.betus@tuke.sk; Tel.: +421-971433352

Abstract

European universities are facing increasingly complex security risks, including physical threats, violence, cyberattacks, emergency situations, and the deterioration of the psychological well-being of students and staff. Rapid societal change, technological development, and increasing uncertainty place mounting pressure on higher education institutions to adopt a systematic approach to the protection of life, health, and property. Despite this, many universities continue to operate through fragmented and largely reactive measures that are insufficiently integrated into a coherent security management system. This paper presents an integrated conceptual framework for security management in higher education institutions, linking physical, cyber, organizational, and psychosocial dimensions of risk governance. By framing university security as a component of institutional sustainability and resilience, the paper situates safety governance within the broader context of sustainable higher education institutions. The framework is grounded in an analysis of existing legislative requirements, the principles of crisis management, and practical experience from the higher education sector. It identifies key sources of risk, core areas of responsibility, and preventive mechanisms that strengthen institutional resilience and emergency preparedness. Particular attention is given to the role of academic staff, institutional leadership, community engagement, and the development of digital security as fundamental pillars of a safe academic environment. By integrating security governance with institutional resilience, the framework supports the sustainable continuity of teaching and research under disruptive events. The proposed framework may serve as a methodological foundation for developing university security strategies and as a tool supporting the long-term organizational and social sustainability of higher education institutions.

Keywords: higher education institutions; sustainability; institutional resilience; security governance; campus safety; risk management; psychosocial well-being; crisis management



Academic Editor: Antonio Caggiano

Received: 11 February 2026

Revised: 4 March 2026

Accepted: 4 March 2026

Published: 6 March 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and

conditions of the [Creative Commons](https://creativecommons.org/licenses/by/4.0/)

[Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

Security is increasingly becoming one of the key priorities of higher education institutions in Europe and worldwide. Universities are directly affected by these developments because they operate as open, densely populated, and highly digitalized environments that combine public accessibility with essential educational and research functions. Recent incidents reported across European and international campuses—including violent

attacks, cyber disruptions targeting learning platforms, and increasing levels of student mental-health distress—illustrate that physical, technological, and psychosocial threats converge in higher education settings. These developments demonstrate that the challenges outlined above are not abstract societal trends but concrete pressures shaping the everyday functioning and governance of universities. Rapid societal change, rising levels of violence, technological advances, and the growth of sophisticated threats are creating new challenges for university governance. Research indicates that the university environment is increasingly exposed to physical, psychological, and technology-driven risks that have a substantial impact on student safety and well-being. A systematic review confirms a high prevalence of gender-based violence in higher education, while empirical studies from the United States indicate a strong association between campus climate and the likelihood of sexual assault and the normalization of sexualized aggression among female students [1–3].

At the same time, new technological threats and prevention tools are emerging that are fundamentally reshaping university security strategies—for example, artificial intelligence systems for weapon detection and early warning [4].

The security of an educational institution can be understood as a condition in which the necessary circumstances are in place to allow it to fulfil its core functions without a real risk of harm to individuals, infrastructure, or institutional reputation. In the context of higher education, security encompasses not only the physical protection of facilities and persons, but also the safeguarding of information systems, the protection of personal data, the prevention of violence and bullying, and the promotion of the psychological well-being of all participants in the educational process.

Empirical studies confirm that inadequate preparedness in the area of fire safety represents a significant risk to students and staff, while weak information risk management increases the vulnerability of university systems to cyber threats [5,6].

At the same time, the role of biometric technologies as tools for controlling access to information in academic environments is becoming increasingly important [7].

The psychological dimension of security is equally critical—research points to the negative impact of bullying and harassment on the mental health of university students, particularly in healthcare-related fields [8].

These findings confirm that the security of higher education institutions is a multidimensional phenomenon that requires a coordinated and systematic approach.

Recent practice has shown a rising frequency of emergency incidents affecting schools and universities, ranging from violent attacks and bomb threats to cyber incidents and public-health-related crises. Research indicates a high prevalence of physical violence among university students and its close association with substance misuse and mental health difficulties [9].

At the same time, the importance of systematic cybersecurity assessment in higher education is increasing, as digital systems have become a critical component of academic infrastructure [10].

Experience from crisis and emergency management highlights the need for a coordinated public-health response to major incidents—one that extends beyond individual institutions and requires integrated mechanisms of inter-organizational cooperation [11].

These findings confirm that fragmented and reactive measures are insufficient to ensure timely risk identification or effective protection of people and infrastructure. International evidence highlights the scale of these challenges. A recent survey by the European University Association reports that 40% of higher education students experience mental-health or well-being difficulties, with approximately one in five facing a mental disorder. Mental-health monitoring across European campuses similarly shows rising levels of anxiety, stress, and burnout among young adults. Cybersecurity reports from ENISA indicate

that cyber incidents targeting higher education institutions have increased substantially in recent years, with ransomware repeatedly identified as one of the most disruptive attack types. Security alerts and documented incidents across several European countries further illustrate that universities are increasingly exposed to physical and psychological violence in their surrounding environments. These trends demonstrate that the most prevalent risks in higher education—psychosocial distress, cyberattacks, and exposure to violence—are recurring issues that directly affect institutional functioning [12–14].

For these reasons, the security of higher education institutions must be understood as an integrated system that combines physical, cyber, organizational, and psychosocial dimensions. Such an approach not only reduces the impact of crisis situations but also supports the systematic development of a culture of prevention, accountability, and cooperation among institutional leadership, academic staff, students, and external partners.

Systematic reviews in the field of information security confirm that user behavior and organizational setting play a decisive role in the overall security posture of universities [15].

At the same time, the growing complexity of cyber threats in academic environments underscores the need to integrate technological, organizational, and human factors into a unified security management framework [16].

The aim of this paper is to propose a conceptual framework for integrated security in higher education institutions that reflects contemporary threats and the evolving needs of the academic environment. The paper is based on an analysis of existing legislative requirements, principles of crisis management, and practical experience from the higher education sector. Its objective is to provide a systematic perspective on security as a strategic component of university governance and to establish a foundation for the further development of preventive and protective measures.

1.1. Contributions of This Paper

This article introduces a novel approach to higher education security by conceptualizing it not as a set of isolated measures, but as an integrated sociotechnical system in which physical, cyber, organizational, and psychosocial risks interact and reinforce one another. While existing approaches typically focus on a single dimension—such as physical protection, cybersecurity, or mental health—universities operate as open and digitally interconnected organizations in which failure in one domain can rapidly escalate into crises in others.

The main scientific and practical contributions of this article are as follows:

1. A four-domain typology of higher education security that systematically integrates physical, cyber, organizational, and psychosocial risk dimensions into a unified analytical framework.
2. A multi-level security governance model that links the strategic level of university leadership, the managerial level of coordination, and the operational level of implementation.
3. Risk-oriented mapping of vulnerabilities and consequences, enabling the identification of how incidents in one domain (e.g., a cyberattack) can propagate into organizational failures or psychosocial crises.
4. Implementation-focused outputs (a risk typology and responsibility mapping) that can serve as a basis for security audits and the development of higher education security strategies.

1.2. Research Questions

To guide the conceptual and analytical development of the proposed integrated security framework, the study is structured around the following research questions:

1. RQ1: How can the key security domains relevant to higher education institutions—physical, cyber, organizational, and psychosocial—be systematically defined and analytically distinguished in a way that reflects contemporary risks and institutional realities?
2. RQ2: What types of threats, vulnerabilities, and cascading effects emerge within and across these four domains, and how do they interact to shape the overall security posture of higher education institutions?
3. RQ3: Which preventive, organizational, and technological measures are currently implemented in higher education institutions, and to what extent are these measures coordinated, integrated, and aligned with regulatory requirements?
4. RQ4: How can the insights from risk mapping, regulatory analysis, and institutional practice be synthesized into a coherent governance framework that supports institutional resilience and sustainable security management?

These research questions provide a structured analytical foundation for the study and ensure that the proposed framework is grounded in a systematic examination of risks, measures, and governance mechanisms across all relevant security domains.

2. Context of Security in the Higher Education Environment

Security in higher education can no longer be understood merely as a technical or administrative issue. It represents a complex domain that affects the everyday functioning of institutions, their relationship with society, and their capacity to respond to evolving risks. Universities today operate in an environment characterized by a high degree of openness, mobility, and technological interconnectedness, which increases their exposure to multiple forms of threat. Research confirms that higher education institutions are among the frequent targets of sophisticated cyberattacks and exhibit significant systemic vulnerabilities [17,18].

At the same time, the nature of threats themselves is changing. Whereas physical risks related to infrastructure and public order once dominated, they are now complemented by cyber incidents, hybrid forms of attack, the spread of disinformation, and psychosocial factors that influence the behavior of individuals and groups. Research shows that students often struggle to reliably identify false or manipulative information and may actively contribute to its further dissemination in digital environments [19,20]. At the same time, evidence confirms that purposefully designed educational interventions can increase resilience to disinformation and strengthen students' critical thinking [21].

Higher education institutions are thus becoming arenas in which security, technological, and social challenges increasingly intersect. Each of these risks is closely linked to specific technological systems that shape the security posture of universities. Physical threats are increasingly managed through access-control technologies, campus surveillance systems, and emergency-notification platforms. Cyber risks are directly connected to the robustness of institutional IT infrastructures, including authentication systems, network segmentation, and backup mechanisms. Psychosocial risks, in turn, are influenced by digital learning environments, online communication channels, and the availability of technology-supported counselling and reporting tools. These technological systems do not eliminate risks, but they significantly influence how effectively universities can detect, prevent, and respond to them.

These changes call for a reassessment of traditional approaches to protection and prevention. Isolated measures that focus on only a single risk domain are no longer capable of providing an adequate level of security. Instead, there is a growing need for an integrated perspective that brings different security dimensions together within a unified management system. Research in higher education management indicates that fragmented information

and governance systems reduce institutions' ability to coordinate processes effectively and respond to crisis situations [22].

Systematic reviews further identify significant challenges in control and governance mechanisms within higher education, highlighting the need for data-driven and strategically integrated solutions [23].

These findings indicate that the contemporary higher education environment is exposed to interconnected threats that go beyond the traditional understanding of security as an isolated technical or organizational issue. Cyber risks, disinformation, psychosocial factors, and crisis situations together create a complex security landscape in which partial and uncoordinated measures are no longer sufficient.

It is therefore essential to move toward an integrated security model that links technological, organizational, and human dimensions within a unified governance system. Such an approach enables not only the early identification of risks but also systematic prevention, coordinated response, and the long-term strengthening of resilience in higher education institutions.

In the context of sustainability, the focus of this study aligns primarily with the social and governance dimensions of institutional sustainability. Security in higher education contributes to social sustainability by safeguarding the well-being, safety, and inclusion of students and staff, while the development of clear responsibilities, coordinated processes, and transparent decision-making strengthens the governance dimension. Although environmental and financial sustainability are not the central focus of this paper, the proposed integrated security framework indirectly supports them by enhancing institutional resilience, reducing the impact of disruptive events, and ensuring the continuity of core academic functions.

Theoretical Foundations: Governance Theory and Its Relevance to Integrated Security

The development of the proposed integrated security framework is grounded in established concepts of governance theory, which provide a structured lens for understanding how complex institutions coordinate decision-making, distribute responsibilities, and manage interdependent risks. Governance theory emphasizes the interplay between hierarchical authority, managerial coordination, and participatory mechanisms, highlighting that effective institutional functioning depends on the alignment of strategic leadership, operational processes, and stakeholder engagement. In the context of higher education, governance frameworks underscore the importance of transparency, accountability, and coordinated action across academic, administrative, and technical units [24].

These principles are directly relevant to security management, as universities operate as multi-actor environments in which physical, cyber, organizational, and psychosocial risks intersect. Governance theory suggests that fragmented or siloed structures reduce institutional capacity to anticipate threats, coordinate preventive measures, and respond to crises. Conversely, integrated governance arrangements—characterized by clear distribution of roles, cross-unit communication, and evidence-based decision-making—enhance institutional resilience and support sustainable security practices. By embedding the proposed security framework within governance theory, the study situates security not merely as a technical function but as a core component of institutional management and long-term sustainability [25,26].

Academic freedom and institutional autonomy constitute essential boundary conditions for any security governance arrangement in higher education. Universities differ from corporate or administrative organizations in that protective measures must not interfere with open inquiry, scholarly communication, or legitimate academic dissent. This requires that security interventions remain proportionate, transparent, and subject to clear

procedural safeguards, ensuring that risk mitigation does not undermine the core academic functions of teaching and research.

3. Materials and Methods

3.1. Research Design

This paper is designed as a conceptual and analytical study aimed at developing a framework for integrated security in higher education institutions. The research design is based on the assumption that security in academic environments constitutes a complex sociotechnical phenomenon that cannot be adequately captured through a single-dimensional empirical approach. Accordingly, the chosen methodology combines a systematic analysis of existing knowledge with practical experience drawn from higher education and security management practice. The analytical process was guided by a set of research questions formulated to structure the identification of security domains, the mapping of risks, and the synthesis of the integrated governance framework. RQ1 guided the conceptual delineation of the four security domains; RQ2 structured the mapping of threats, vulnerabilities, and cascading effects; RQ3 informed the analysis of existing preventive, organizational, and technological measures; and RQ4 directed the synthesis of these insights into the proposed integrated governance framework.

The purpose of this design is to identify the key dimensions of security, their interrelationships, and critical points of vulnerability, which subsequently form the basis for the development of an integrated security management framework.

To provide methodological clarity, the study adopts an integrative review approach that synthesizes scholarly literature, regulatory frameworks, and institutional practice into a coherent analytical basis for framework development. This approach does not constitute a systematic review in the PRISMA sense; rather, it is designed to identify recurring patterns, conceptual categories, and governance-relevant insights across heterogeneous sources. The literature synthesis is complemented by a structured document analysis of internal university materials, enabling the triangulation of academic knowledge with practical security arrangements. Together, these elements form a transparent and replicable conceptual methodology suitable for developing an integrated security governance framework.

The methodological approach used in this study corresponds to a narrative integrative review, selected to support framework development in a field where relevant evidence is distributed across academic research, regulatory requirements, and institutional practice. Accordingly, the synthesis intentionally combined three complementary source streams—peer-reviewed literature, normative and policy documents, and anonymised internal university materials—because the governance of security in higher education is shaped not only by empirical findings but also by legal obligations and operational arrangements.

The framework was developed through an iterative, stepwise synthesis process. Firstly, the analytical scope and core dimensions of security governance were defined in line with RQ1–RQ4. Secondly, concepts, obligations, and recurring control mechanisms were extracted from each source stream and consolidated into a shared set of categories. Thirdly, these categories were organised into the four-domain structure and mapped to governance levels (strategic, managerial, operational) to clarify roles, processes, and interfaces. Finally, the resulting structure was refined by checking internal consistency across domains and by verifying that each framework element could be traced back to at least one of the source streams.

In this context, database searching served as an entry point for scholarly evidence, while regulatory and institutional materials were incorporated through targeted retrieval and document-based analysis to ensure coverage of the normative and operational aspects required for a coherent governance framework.

3.2. Data Sources and Material

Three main types of sources were used as input material. These source categories were identified through the structured search process described in Section 3.2.1, which outlines the databases, keywords, and selection criteria used to retrieve relevant materials.

The scope differs across the three source categories because each type of material is defined by a different methodological boundary: scholarly literature is delimited by publication years, whereas normative documents and institutional practice are delimited by their geographical and regulatory relevance.

1. Scholarly and professional literature from the fields of higher education security, cybersecurity, crisis and emergency management, psychological safety and student well-being, and organizational and public administration management. This body of literature included studies addressing technological, organizational, and psychosocial aspects of security, including research on the adoption of campus IoT systems and privacy protection in academic environments, mechanisms for preventing psychological crises and suicidality among students, and comparative analyses of institutional policies on artificial intelligence and education governance [27–29].
2. Normative and regulatory documents defining requirements for security, data protection, crisis planning, and risk prevention in higher education institutions. These included in particular national and European frameworks, recommendations, and guidelines governing information security, personal data protection, emergency management, and health protection in academic settings.
3. Content analysis of existing internal security frameworks and procedures, developed in the original professional source text that served as the empirical and applied foundation for this study. This material made it possible to identify typical organizational and procedural arrangements used in higher education institutions and to examine their alignment with the proposed conceptual framework of integrated security.

3.2.1. Search Strategy and Selection

As this study is conceptual and analytical in nature and is based on a synthesis of existing knowledge, the literature search was conducted as a transparent and reproducible process. Although the search was conducted in a structured and reproducible manner, it was not designed as a formal PRISMA protocol, as the study follows a conceptual and integrative analytical approach. The objective was to identify core sources relevant to higher education security across the four domains—physical, cyber, organizational, and psychosocial—while also capturing the intersections between them. Table 1 provides an overview of the three categories of sources retrieved through this search strategy.

Table 1. Data sources and selection (elaborated by authors).

Source Type	Content	Original Time Period	Geographical Scope
Scholarly literature	Peer-reviewed studies on campus security, cybersecurity, crisis management, and student mental health	2019–2026	International (English-language literature)
Normative and regulatory documents	Higher education legislation, personal data protection laws, crisis management frameworks, GDPR, and national and European security regulations	Not time-delimited (validity based on current legal framework)	European Union; Slovak Republic
Institutional practice	Security projects, facility protection plans, crisis and evacuation procedures, and the prevention of violence and cyber threats	2019–2025	Slovak higher education institutions; anonymized internal documentation

Databases and search strategy. The literature search was conducted in Scopus and Web of Science, with supplementary searches via Google Scholar to identify cited and related works.

Combinations of English-language keywords were used, for example: (*“higher education” OR university OR campus*) AND (*security OR safety OR “risk management” OR resilience*):

- Domain-specific thematic branches were defined as follows;
- Physical: (*violence OR “emergency preparedness” OR “access control” OR evacuation*);
- Cyber: (*cybersecurity OR ransomware OR “data breach” OR LMS*);
- Organizational: (*governance OR policy OR “crisis management” OR coordination*);
- Psychosocial: (*“mental health” OR bullying OR harassment OR wellbeing OR “psychosocial support”*).

Time frame and language. Publications from 2019 to 2026 were included, primarily in the English language.

Inclusion and exclusion criteria.

Included were:

- Peer-reviewed articles, systematic reviews, and relevant empirical studies in higher education;
- Works with a clear link to at least one of the four domains;
- Sources addressing risk management, incident management, or security measures in higher education.

Excluded were:

- Studies not related to higher education (e.g., those focusing exclusively on primary or secondary education);
- Duplicates;
- Texts without full-text availability or without a clearly identifiable methodology.

Screening and selection.

The selection process followed three steps:

1. Title and abstract screening;
2. Full-text assessment;
3. Supplementation of sources through backward and forward snowballing (citation tracking).

The final set of sources was then thematically mapped to the domains and used in the analytical steps of the study (risk mapping → measures → framework synthesis).

3.2.2. Regulatory and Normative Mapping

This mapping table shows that legislative and regulatory requirements do not apply to isolated areas but instead create an obligation for higher education institutions to manage security as an interconnected system. GDPR and cybersecurity regulations are primarily linked to the cyber and organizational domains, while occupational health and safety and fire protection are mainly physical in nature but require strong organizational arrangements. Measures against discrimination and bullying, in turn, explicitly embed psychosocial security as a component of institutional governance.

Although the regulatory mapping presented in this section focuses on the European Union and the Slovak national framework, the proposed integrated security model is not limited to these contexts. Higher education systems operate under diverse governance and management arrangements, ranging from centralized regulatory regimes to decentralized, institution-driven models such as those found in the United States, the United Kingdom, or the Nordic countries. Despite these structural differences, the core principles of the framework—cross-domain coordination, clear allocation of responsibilities, and evidence-based decision-making—remain applicable across systems. The model is compatible with both standardized management architectures (e.g., risk management, information security, business continuity systems) and internally developed institutional procedures, allowing it to function within varying degrees of institutional autonomy and regulatory density.

The regulatory and normative requirements relevant to the four security domains are summarised in Table 2.

Table 2. Mapping of regulatory and normative requirements to security domains (elaborated by authors).

Regulatory/Normative Requirement	Relevance for HE	Security Domain(s)	Examples of Required or Implied Measures
GDPR (EU 2016/679) [30]	Protection of personal data of students and staff	Cyber, Organizational	access control, data minimisation, incident reporting, DPO, staff training
NIS2 Directive/national cybersecurity law	Protection of critical and important digital services (incl. HE IT systems)	Cyber, Organizational	risk management, incident response, security monitoring, backups
Occupational Health and Safety (OHS)/Fire safety (BOZP, PO)	Safety of students and employees on campus	Physical, Organizational	evacuation plans, drills, fire protection systems
Higher Education Act (national)	Institutional responsibility for safe learning environment	Organizational, Psychosocial	internal regulations, disciplinary procedures, student protection
Anti-discrimination and anti-harassment legislation	Protection against bullying, harassment, violence	Psychosocial, Organizational	reporting channels, investigation procedures, counselling
Crisis management/civil protection regulations	Preparedness for emergencies and extraordinary events	Physical, Organizational	crisis teams, emergency plans, communication protocols

3.2.3. Institutional Practice and Document Analysis

The institutional practice component of the study was based on the analysis of internal security-related documents from several higher education institutions operating within the same national regulatory framework. To protect institutional confidentiality and sensitive information, all documents were fully anonymised and are referenced only by type, not by institution.

The analysed material consisted of formal internal documents typically used by universities for safety and risk management, including crisis and emergency plans, physical security and access control policies, IT and cybersecurity policies, data protection and GDPR-related procedures, codes of conduct and anti-harassment policies, and student support and crisis intervention frameworks.

In total, the corpus included dozens of documents produced between 2019 and 2025, reflecting both pre-pandemic and post-pandemic security arrangements. No personal data or identifiable information were processed in this study. The institutional practice material used in this study is summarised in Table 3.

Table 3. Overview of institutional practice material (elaborated by authors).

Type of Document	Typical Content	Main Security Domain(s)
Crisis and emergency plans	evacuation, crisis teams, communication	Physical, Organizational
Physical security policies	access control, CCTV, guards	Physical
IT and cybersecurity policies	data protection, incident response, backups	Cyber
Codes of conduct, anti-harassment	reporting, investigation, sanctions	Psychosocial, Organizational
Student support and counselling frameworks	crisis intervention, wellbeing	Psychosocial

The documents were analysed using a thematic coding approach, focusing on four categories:

1. Types of risks addressed;
2. Prescribed preventive and reactive measures;
3. Allocation of responsibilities;
4. Links to regulatory or legal requirements.

These themes were then mapped to the four security domains and used as an applied foundation for the construction of Table 4 (risk typology), Table 5 (RACI responsibilities), and Figure 1 (governance framework).

3.3. Analytical Procedure

To strengthen the analytical precision of the study, the reviewed literature, regulatory documents, and institutional materials were subjected to a basic content-oriented coding process. Recurring concepts, risk categories, and governance-related themes were identified through repeated reading and grouped into higher-order thematic clusters. This form of qualitative content structuring was used not to quantify the frequency of themes, but to ensure that the typology of risks and the governance framework reflect the most consistently recurring patterns across the reviewed sources.

The analytical procedure consisted of four consecutive steps:

Step 1—Identification of security domains

Based on the literature and existing approaches, four main security domains were identified:

- Physical security;
- Cybersecurity;
- Organizational security;
- Psychosocial security.

These domains were considered the fundamental pillars of security in higher education institutions. This step corresponds to RQ1, which focuses on defining and analytically distinguishing the key security domains relevant to higher education institutions.

Step 2—Risk mapping

For each domain, typical threats, vulnerabilities, and potential impacts were identified. The mapping was based on a combination of:

- Published empirical studies;
- Reports on incidents in university environments;
- Practical experience in security management.

In this study, reports on incidents in university environments refer to publicly available university alerts and official incident summaries (e.g., bomb threats, evacuations, cyber incidents), used only at an aggregated level without institutional identifiers. This analytical step addresses RQ2 by identifying threats, vulnerabilities, and cascading effects within and across the four security domains.

Step 3—Analysis of existing measures

Typical preventive, technical, and organizational measures used in higher education institutions were then analysed. Particular attention was paid to the extent to which these measures are:

- Coordinated;
- Systematically managed;
- Interconnected across domains.

This step responds to RQ3 by examining the preventive, organizational, and technological measures currently implemented in higher education institutions and assessing their level of coordination and integration.

Step 4—Framework synthesis

The results of the previous steps were synthesized into a proposed integrated security framework that links individual domains, actors, and processes into a unified system. This step directly addresses RQ4 by integrating the insights from the previous analytical phases into a coherent governance framework for institutional security and resilience.

3.4. Outputs of the Methodology

The methodological procedure resulted in three main outputs:

- A typology of security risks relevant to higher education institutions;
- A mapping of actors and responsibilities in the area of security;
- A conceptual model of integrated security, which is presented in the following section of the article.

These outputs are presented in the form of:

- Tables;
- Diagrams;
- A systematic textual exposition.

Together, these methodological outputs provide structured answers to RQ1–RQ4 by defining the security domains, mapping cross-domain risks, analysing existing measures, and synthesizing these insights into the integrated security framework.

4. Results

The synthesis of risks, responsibilities, and institutional processes is informed by empirical and regulatory analysis, as well as by governance theory, which provides a conceptual basis for integrating diverse security domains into a coherent institutional framework.

Because this study is conceptual and analytical in nature, the Results Section synthesizes insights from the reviewed literature, regulatory frameworks, and institutional practice documents. References are included to demonstrate how existing evidence and practice inform the construction of the integrated security framework, rather than to present new empirical findings.

The framework and role allocations presented below represent an author-derived synthesis of the reviewed sources and regulatory requirements, intended as a conceptual reference model.

4.1. Typology of Security Risks in the Higher Education Environment

This subsection presents the findings related to RQ1, which focuses on defining and analytically distinguishing the key security domains relevant to higher education institutions. Security risks in higher education cannot be reduced to individual isolated incidents. They form a dynamic system of threats that interact with and reinforce one another within the everyday operation of universities. The synthesis of the literature and applied experience indicates that these risks can be meaningfully grouped into four main domains: physical, cyber, organizational, and psychosocial security. These domains serve as analytical categories that allow the diversity of threats and their impacts on the academic environment to be examined in a systematic manner.

The physical dimension of security encompasses the protection of people and infrastructure against violence, accidents, and emergency events. The open character of university campuses, high levels of population turnover, and extensive physical spaces create specific vulnerabilities that distinguish them from other types of organizations. Research in campus security highlights the importance of access control, biometric technologies, and the digital transformation of security systems as tools for reducing these vulnerabilities [31].

Incidents such as violent attacks, fires, or unauthorized intrusions have immediate and often highly visible effects on institutional operations, including the disruption of

teaching, evacuations, and the erosion of the sense of safety within the academic community. Empirical studies further demonstrate that the level of preparedness of students and staff significantly influences universities' capacity to manage such situations effectively [32].

The cyber dimension has in recent years become as critical as physical security. Digital platforms, learning management systems, academic databases, and administrative information systems constitute the core operational environment of universities. Disruptions to these systems—whether through data breaches, ransomware, or attacks on service availability—can have long-term consequences not only for institutional operations but also for the trust of students and external partners.

Current research in cyber-physical systems and the Internet of Things highlights the high level of vulnerability of complex digital infrastructures and the need for advanced risk assessment and threat detection methods capable of identifying hidden and gradually accumulating attacks [33,34].

The organizational dimension of security represents a less visible, yet often decisive component of risk management. It encompasses the quality of decision-making processes, the clarity of responsibilities, the availability of crisis plans, and the institution's capacity to coordinate responses across different units. Research on the resilience of educational environments highlights the importance of organizational adaptability, digital tools, and strategic governance in managing crises and disruptions to teaching [35].

Empirical studies from higher education further show that the level of institutional preparedness for emergencies, such as natural disasters, significantly affects the ability to maintain educational continuity and minimize damage [36].

Systematic training and exercises in crisis management also play a crucial role in improving coordination and decision-making under critical conditions [37].

Failures in this domain can substantially amplify the impacts of otherwise manageable incidents, for example through delayed communication or unclear command structures during a crisis.

The psychosocial dimension concerns mental well-being, interpersonal relationships, and the overall climate within the academic environment. Prolonged stress, bullying, social isolation, and academic pressure can weaken the resilience of individuals and groups alike, increasing the risk of conflict escalation and crisis situations. Research indicates that academic and cultural stressors, language barriers, discrimination, and insufficient institutional support significantly contribute to anxiety, depressive symptoms, and social isolation among students [38].

Empirical models further show that academic stress and cognitive appraisals of situations directly affect students' levels of anxiety and self-esteem, while the use of digital and AI-based tools may further mediate this relationship through feelings of loneliness [39,40].

Systematic reviews confirm that poor adaptation to the higher education environment leads to increased stress, burnout, and a higher risk of academic failure or early withdrawal from studies [41]. At the same time, supportive networks, organizational skills, and targeted interventions significantly enhance psychological resilience and students' capacity to cope with demands [42].

This dimension is therefore directly linked to the prevention of violence and to the ability of the academic community to respond to threats in a constructive manner.

The results of the analysis indicate that these four domains cannot be understood in isolation. In practice, physical, digital, organizational, and psychosocial factors reinforce one another, creating a complex security environment that requires an integrated approach to risk management.

For the purpose of systematic comparison and analysis of security threats in the higher education environment, a detailed risk typology was developed based on the four core

domains identified in the previous section. This typology makes it possible to capture not only the threats themselves, but also their associated vulnerabilities and potential consequences for institutional operations.

Table 4 summarizes the main categories of security risks, typical examples of threats, and the areas in which universities tend to be most vulnerable. The purpose of this overview is not to produce an exhaustive list of all possible incidents, but to provide an analytical framework that helps to capture the complexity of the security environment and to identify critical points on which preventive and protective measures should be focused.

Table 4. A Detailed Typology of Security Risks in Higher Education Institutions (elaborated by authors).

Domain	Risk Type	Examples of Threats	Typical Vulnerabilities	Possible Consequences	Indicators/Warning Signs	Typical Control Measures
Physical	Violence	physical assaults, threats, armed incidents	open campus, weak supervision, uncontrolled access	injuries, trauma, evacuations, disruption of teaching	increased reports of aggression, access breaches, CCTV incidents	access control, CCTV systems, security staff, emergency buttons, regular drills
Physical	Accidents	fires, injuries, technical failures	ageing buildings, poor maintenance	health damage, closure of facilities	frequent malfunctions, safety violations	fire alarms, inspections, evacuation plans, training
Physical	Unauthorized access	intrusion into buildings	weak identification of persons	theft, endangerment of people	unknown individuals on premises	access cards, biometrics, reception
Cyber	Data breaches	theft of personal data	weak passwords, phishing	loss of trust, GDPR penalties	suspicious logins, data leaks	MFA, staff training, DLP
Cyber	Ransomware	system lockouts	unpatched systems	suspension of teaching, data loss	LMS outages, ransom messages	backups, patching, incident response plans
Cyber	Sabotage	DDoS attacks, LMS attacks	centralized IT infrastructure	disruption, service outages	slow or unavailable systems	network segmentation, monitoring
Organizational	Governance failure	unclear command structures	lack of plans	delayed responses	communication chaos	crisis teams, RACI matrices, crisis manuals
Organizational	Communication failures	incorrect or inconsistent information	weak crisis communication channels	panic, disorganization	spread of rumours	official communication channels, spokesperson
Psychosocial	Stress	burnout, overload	excessive demands	reduced performance	absenteeism, burnout	counselling services, work–life balance policies
Psychosocial	Bullying	mobbing, harassment	weak reporting mechanisms	conflict, anxiety	complaints, isolation	anonymous reporting, interventions
Psychosocial	Social isolation	loneliness	lack of support	crises, dropout	disengagement, absenteeism	mentoring, psychological support

Note: Table 4 synthesises risks and controls identified through the combined analysis of peer-reviewed literature, regulatory and normative requirements, and anonymised institutional practice documents, as described in Section 3. Abbreviations: MFA—multi-factor authentication; DLP—data loss prevention; LMS—learning management system; RACI—Responsible, Accountable, Consulted, Informed.

The extended typology presented in Table 4 does not describe only the types of threats, but also their early indicators and typical control measures, thereby linking risk identification with the practical management of security in higher education institutions.

4.2. Risk and Vulnerability Mapping

This subsection addresses RQ2 by mapping threats, vulnerabilities, and cascading effects across the four security domains. Security risks in higher education do not arise in isolation but emerge from the interaction between the environment, technology, organizational structures, and people. The results of the analysis show that the same event can have different impacts depending on the institution's level of preparedness, available resources, and the quality of governance. Research indicates that teachers' occupational well-being and self-efficacy, as well as the quality of their relationships with students and colleagues, significantly influence the capacity of educational institutions to cope with stressful situations and maintain stability during crises [43].

In the case of physical incidents, the open architecture of university campuses and high levels of population turnover play a decisive role, increasing the likelihood of unauthorized access and complicating the early detection of threats. Cyber threats, by contrast, are characterized by their invisibility and their capacity to disrupt critical systems without the attacker's physical presence. Contemporary studies on digital responsibility and the management of technological challenges among public administration students show that low levels of digital competence and risk awareness can significantly increase institutional vulnerability to cyber incidents [44].

Organizational vulnerabilities are manifested primarily in the form of unclear responsibilities, missing crisis plans, and weak communication channels. Empirical research in higher education indicates that the ability of students and staff to balance academic, organizational, and personal demands plays a significant role in maintaining institutional functionality during periods of strain [45].

Psychosocial factors, such as prolonged stress or isolation, can further reduce individuals' capacity to respond rationally and increase the risk of conflict escalation.

These layers of vulnerability overlap and form complex risk profiles that require a systemic and integrated approach to security management. Conceptual approaches to security and social protection in education emphasize the importance of linking institutional policies, financial mechanisms, and support services in building the resilience of academic communities [46].

4.3. Mapping of Responsibilities Within Integrated Security

This subsection responds to RQ3 by examining how preventive, organizational, and technological measures are allocated and coordinated across institutional actors.

The RACI classifications in Table 5 were established through a conceptual synthesis of widely used governance models and publicly available regulatory requirements relevant to higher education institutions. The allocation of responsibilities reflects general patterns found in standard university governance structures, including legally defined roles such as the Data Protection Officer under GDPR. No identifiable or sensitive institutional data were used; the matrix represents a generalized model derived from common organisational practices rather than from any specific institution.

Role definitions:

University leadership refers to the rectorate or senior management responsible for strategic decisions.

Security management denotes the organisational unit or designated security officer responsible for coordinating physical and organisational security.

IT services cover institutional information systems and cybersecurity.

Student support services include counselling, psychological and social support.

Data Protection Officer (DPO) is the legally required role under GDPR responsible for data protection oversight.

Communication/PR is responsible for internal and external crisis communication.

This responsibility map demonstrates that higher education security cannot be delegated to a single unit, but requires coordination among university leadership, security and IT functions, and actors working directly with students. The model makes it possible to clearly identify who makes decisions, who carries out actions, and who provides support across the different security domains.

Table 5. RACI Matrix for Security Management in Higher Education Institutions (elaborated by authors).

Security Area	University Leadership	Security Management	IT Services	Academic Staff	Student Support Services	Data Protection Officer (DPO)	Communication/PR
Physical security (access control, CCTV, guards, evacuation)	A	R	I	C	I	I	I
Cybersecurity and IT continuity	A	C	R	I	I	C	I
Data protection and GDPR compliance	A	C	C	I	I	R	I
Crisis and emergency management	A	R	C	C	C	I	C
Violence prevention and incident reporting	A	C	I	R	C	I	I
Psychosocial support and crisis intervention	A	I	I	C	R	I	I
Crisis communication (internal and external)	A	C	I	I	C	I	R

Note: R = Responsible; A = Accountable; C = Consulted; I = Informed.

4.4. Actors and Responsibilities in the Integrated Security System

The analysis presented in this subsection further elaborates the findings related to RQ3 by clarifying the distribution of roles and responsibilities within the integrated security system. Effective security management in higher education depends on a clear allocation of roles and responsibilities among the various actors. The results of the analysis show that even where robust technical and organizational measures exist, failures of coordination or unclear competences can significantly reduce an institution's ability to respond to crisis situations.

A university's security system operates across multiple levels of governance. At the strategic level, university leadership plays a central role by defining security policy, approving crisis plans, and allocating resources. At the tactical level, specialized units—such as security departments, IT services, student affairs offices, and crisis teams—are responsible for implementing measures and coordinating responses. The operational level consists of academic staff, administrative personnel, and students themselves, who are often the first to detect threats or become directly involved in incidents.

The interconnection of these levels is critical to the functioning of the system as a whole. In the absence of clear vertical and horizontal communication, information about threats may be delayed or lost, increasing the risk of escalation. Equally important is the ability of individual actors to understand their role in a crisis and to know which actions to take.

Particular attention must be given to the involvement of students and academic staff in security processes. These actors are not merely passive recipients of protection but active components of the system who can contribute to the early identification of risks, the prevention of conflict, and the promotion of a safe academic culture. Their level of awareness, trust in the institution, and willingness to cooperate significantly influences the overall effectiveness of security measures.

An integrated approach to security therefore requires not only technical solutions, but also the systematic development of capacities, clear governance processes, and a culture of cooperation among all actors within the university environment.

4.5. Conceptual Framework of Integrated Security

This subsection synthesizes the insights corresponding to RQ4 by presenting the integrated governance framework derived from the preceding analytical steps. Based on the results of the preceding analyses, a conceptual framework of integrated security has been developed that links physical, cyber, organizational, and psychosocial dimensions into a unified system of governance. This framework is grounded in the premise that the security of higher education institutions cannot be ensured through isolated measures, but only through a coordinated and systematic approach.

The proposed framework is structured around three core layers. The first is the operational layer, which comprises concrete technical, human, and procedural measures—such as access control, IT security, crisis planning, and psychological support. The second is the management layer, which encompasses decision-making processes, defined responsibilities, communication, and coordination across institutional units. The third is the strategic layer, within which security policies, priorities, and long-term institutional objectives are formulated.

A key feature of the framework is the interconnection of these layers. Information on incidents, risks, and emerging needs at the operational level must be effectively transmitted to the management and strategic levels, where it is translated into decisions and corrective actions. At the same time, strategic direction must create the conditions necessary for the effective functioning of operational processes.

The framework also emphasizes the role of feedback and learning from incidents. Each emergency or security problem constitutes a source of knowledge that should be systematically analysed and used to improve security practices and policies.

Because certain security measures may affect academic work or stakeholder relationships, the framework incorporates governance safeguards such as proportionality assessment, consultation with affected academic units, and role separation between operational implementation and oversight. These mechanisms help ensure that security interventions remain compatible with academic freedom, privacy obligations, and institutional ethics.

The integrated security framework also aligns with established sustainability assessment systems used in higher education. Several components of the model correspond directly to ESG criteria: physical and psychosocial safety contribute to the social dimension (S), cybersecurity and governance structures reinforce institutional accountability and transparency within the governance dimension (G), and risk-management processes support long-term operational resilience. The framework is likewise compatible with sustainability indicator sets commonly applied in HEIs, such as STARS and UI GreenMetric, which include metrics related to campus safety, emergency preparedness, data protection, well-being, and governance performance. In terms of the Sustainable Development Goals, the framework contributes most directly to SDG 3 (Good Health and Well-Being), SDG 4 (Quality Education), SDG 11 (Sustainable Cities and Communities), and SDG 16 (Peace, Justice and Strong Institutions) by strengthening institutional resilience, safeguarding learning continuity, and promoting safe and inclusive academic environments.

Graphical Model of the Integrated Security Framework

To facilitate a clearer understanding of the relationships between the individual domains and governance levels, the proposed conceptual framework is illustrated graphically in Figure 1. The model depicts the four security domains—physical, cyber, organizational,

and psychosocial—as the foundational layers of the university security environment and shows their links to operational, managerial, and strategic processes.



Figure 1. Integrated security framework of higher education institutions showing the interaction between security domains, operational processes, management coordination, and strategic governance (elaborated by authors).

At the core of the model are the security domains, which represent the areas in which risks emerge and concrete protective measures are implemented. Above them lies the operational layer, encompassing everyday preventive and response mechanisms such as technical safeguards, IT security tools, crisis procedures, and support services. The management layer provides coordination, decision-making, and information flows among actors and organizational units. The strategic layer defines the long-term direction of security policy, as well as the allocation of institutional resources and priorities.

Figure 1 also illustrates the feedback loops between the different levels, enabling the system to learn from incidents and adapt to a changing risk environment.

4.6. Scenario-Based Illustration of Framework Application

This scenario-based illustration provides an applied demonstration of the framework developed in response to RQ4. The purpose of the following scenario-based analysis is not to statistically validate the proposed framework, but to demonstrate its operational coherence and practical applicability in a complex, multi-domain crisis situation typical for higher education institutions.

Scenario: During the examination period, a university faces a combined threat—a bomb threat accompanied by a simultaneous outage of the learning management system (LMS) as a result of a cyberattack.

Physical domain: The threat requires the immediate evacuation of buildings, access control measures, and intervention by security services.

Cyber domain: The LMS outage prevents communication with students and access to examination materials, thereby increasing confusion and the risk of disinformation.

Organizational domain: A crisis management team is activated to coordinate security, IT, and communication measures. A failure to clearly allocate responsibilities would lead to delayed responses.

Psychosocial domain: Students and staff experience heightened anxiety, panic, and the spread of rumours, increasing the risk of undesirable behaviour and disruption of academic activities.

Applying the proposed framework in this scenario makes it possible to systematically integrate physical, digital, organizational, and psychosocial measures. While an isolated approach would address each incident separately, the integrated model supports coordinated action, clear command structures, and the parallel activation of security, IT, and support services.

This example demonstrates that the framework is not merely a theoretical construct but can also serve as a practical tool for planning and managing complex crisis situations in higher education institutions.

This scenario-based illustration provides an initial plausibility check of the framework and supports its use as a structured tool for security planning, while further empirical validation remains a task for future research.

5. Discussion

This discussion interprets the findings in relation to RQ1–RQ4, highlighting how the proposed framework addresses the conceptual, analytical, and governance-related dimensions of integrated security in higher education institutions. The proposed integrated security framework highlights the need to move beyond fragmented approaches to protecting higher education institutions. The findings of this study show that many existing policies and measures focus on individual dimensions of security—such as the physical protection of buildings or cybersecurity—without systematically addressing their interconnections.

The literature on higher education management and security repeatedly demonstrates that isolated solutions have limited effectiveness in environments where physical, digital, and psychosocial factors interact. The proposed framework extends these approaches by explicitly integrating technological, organizational, and human elements into a single governance system.

The organizational layer is of particular importance, as it is often treated only marginally in existing models. The results indicate that the quality of governance, communication, and coordination can decisively determine whether a security incident remains a manageable event or escalates into a major crisis.

Equally important is the psychosocial dimension, which is frequently underestimated in technically oriented security models. This study shows that mental well-being, interpersonal relationships, and trust in the institution are not merely “soft factors” but fundamental components of resilience in the university environment.

5.1. Comparison with Existing Approaches

The analysis presented in this subsection relates primarily to RQ4, as it positions the proposed integrated framework within the context of existing approaches and demonstrates how it synthesizes insights across the four security domains. The proposed integrated security framework differs in several key respects from most approaches described in the existing literature. A large proportion of research focuses either on technical aspects of security—such as cybersecurity and digital infrastructure—or on individual risk dimensions, including physical incidents or student mental health. For example, studies in higher education management emphasize the role of cybersecurity as a means of enhancing institutional performance and protecting digital assets, while other research concentrates primarily on cybersecurity education and the development of individual competencies through training and gamification [47–49].

Systematic reviews in the higher education context further show that research attention is often directed toward technical and information security practices, with limited integration of organizational and psychosocial dimensions of security [50].

While these approaches provide valuable insights, they frequently remain fragmented and fail to offer a comprehensive understanding of how different risks within higher education environments interact.

Studies focusing on digital security and technological systems typically analyse vulnerabilities in IT infrastructures, the risks of data breaches, and attacks on learning manage-

ment systems. For example, research on the monitoring of computer activity in academic environments concentrates primarily on technical architectures, data collection, and the control of user activities as tools for securing teaching processes and preventing misuse [51].

Similarly, studies on data breach incidents often focus on the maturity of data governance and users' risk perceptions, with the primary emphasis placed on data management systems and processes [52].

While these works provide detailed technical and analytical solutions, they rarely connect them to the organizational processes and human factors that ultimately determine how such technologies are used and protected in practice. The proposed framework addresses this gap by situating cybersecurity within a broader context of governance, competencies, and stakeholder education.

Similarly, research oriented toward the psychosocial aspects of security tends to focus on stress, bullying, mental health, and students' academic adjustment. These studies convincingly demonstrate that psychological well-being and social climate have a direct influence on the occurrence of conflict, risk-taking behaviour, and crisis situations. Empirical research in higher education shows that academic pressure, language and cultural barriers, discrimination, and inadequate institutional support significantly contribute to students' anxiety, social isolation, and depressive symptoms [38].

Quantitative models further confirm strong relationships between academic stress, cognitive appraisals of situations, and levels of anxiety, while digital environments and technology use can further mediate these relationships through feelings of loneliness [39,40].

Systematic literature reviews also indicate that poor adaptation to the higher education environment increases the risk of burnout, psychological strain, and academic failure, whereas the presence of support networks and the development of resilience significantly improve students' ability to cope with demanding situations [41,42].

In existing models, however, these psychosocial factors are typically analysed largely in isolation from technical and organizational protection mechanisms. By contrast, the integrated framework treats them as equal pillars of security and explicitly links them to crisis management and risk prevention.

A further important contribution of the proposed approach lies in its emphasis on multi-level security governance—from operational processes to strategic decision-making. Many existing approaches are limited to describing individual measures or policies, whereas the model proposed here systematically connects everyday practice with long-term planning and resource allocation. Research on digital transformation and the implementation of artificial intelligence in higher education highlights the need to align technological solutions with institutional strategies, evaluation mechanisms, and organizational processes in order to ensure their sustainability and safe use [53].

Similarly, work in the field of research security and integrity emphasizes that the protection of academic systems, data, and knowledge cannot be achieved solely through isolated rules, but requires the systematic integration of ethical, legal, and managerial frameworks across the institution as a whole [54].

5.2. Implications for University Governance and Policy

The implications discussed in this subsection further elaborate the findings related to RQ4 by demonstrating how the integrated framework can guide institutional governance, policy development, and strategic decision-making. The proposed integrated security framework has significant implications for how universities approach security governance. Rather than maintaining separate policies for physical protection, IT security, or student support, the framework emphasizes the need for a unified strategy that links these areas into a coherent system. Such an approach enables better coordination, more

efficient use of resources, and more consistent decision-making in both crisis situations and routine operations.

Research on digital responsibility and the governance of public institutions shows that the ability to integrate technological, organizational, and ethical dimensions of management is critical for the sustainability and security of academic environments (Cuares & Casaña, 2026) [44]. Similarly, analyses of higher education transformation in the context of globalization emphasize the need for system-level, value-based governance that goes beyond isolated policy or technical measures [55].

Empirical studies in higher education further confirm that integrated approaches to risk management improve project performance and institutional resilience compared to fragmented governance models [56].

From a policy-making perspective, an integrated approach implies the need to align security strategies with academic objectives, digitalization initiatives, and student support policies. Security should not be viewed as a barrier to innovation or openness, but as a prerequisite for their sustainable development. This is particularly important in an environment characterized by growing demands for online education, the use of artificial intelligence, and international student mobility.

Research on the digital transformation of higher education indicates that modern enterprise IT systems and integrated digital strategies are essential conditions for the secure and efficient operation of educational institutions [57].

At the same time, analyses of the impact of artificial intelligence on the role of university teachers show that technological innovation is fundamentally reshaping pedagogical and organizational processes, thereby increasing the need to systematically integrate security and ethical considerations into university governance [58].

At the institutional level, implementing the integrated framework requires a clear definition of responsibilities, the establishment of cross-functional crisis teams, and systematic training for staff and students. Without adequate organizational anchoring, even the most advanced technical solutions remain underutilized or improperly applied. Research in human resource management and digital transformation indicates that organizations' ability to make effective use of new technologies, including artificial intelligence, depends on levels of preparedness, competence, and employee engagement, particularly among younger generations entering the academic environment [59].

Empirical studies in higher education also show that systematic training in crisis management and preparedness significantly improves institutions' capacity to coordinate responses to emergency situations and to mitigate their negative impacts.

An integrated approach also enables more effective risk assessment and priority setting. By linking data from physical security, cyber incidents, and psychosocial indicators, institutions can develop more accurate risk profiles and direct preventive measures to where they are most needed. Research on cyber vulnerability assessment and threat detection highlights the importance of combining multiple data sources and analytical methods to identify hidden and cumulative risks in complex systems [33,34].

At the same time, empirical models of academic stress, loneliness, and mental well-being show that psychosocial indicators can serve as early warning signals of rising risks of conflict and crisis situations [39,40].

Integrating these types of data thus enables universities to move from reactive incident handling toward proactive security management.

5.3. Limitations of the Study

The limitations outlined in this subsection clarify the scope within which RQ1–RQ4 were addressed and identify areas where future empirical research is needed to validate

and operationalize the proposed framework. The chosen approach is based on a synthesis of the literature and applied experience rather than on primary empirical data collection. Accordingly, the proposed framework should be understood as a conceptual and analytical contribution that provides an integrative governance model and structured instruments for application in future empirical, institutional, or comparative studies. While this limits statistical generalization, it enables a comprehensive synthesis of regulatory, organizational, and psychosocial dimensions that are often examined separately in empirical research.

The proposed framework does not yet include operational key performance indicators or benchmarking metrics that would allow institutions to systematically assess implementation progress or compare security maturity across units. As the present study is conceptual in nature, the development of measurable indicators falls outside its scope. However, the structure of the framework enables the future creation of KPIs related to incident response capacity, cross-unit coordination, training coverage, system reliability, and psychosocial support effectiveness. The incorporation of such metrics is therefore identified as an important direction for subsequent empirical and applied research.

The framework also does not examine how specific security measures may influence academic freedom or stakeholder trust across different institutional cultures. These dynamics represent an important direction for future research, particularly in comparative studies of security governance in higher education.

6. Conclusions

An integrated approach to higher education security represents a necessary shift from fragmented and reactive measures toward systematic and preventive risk management. The findings of this study confirm that the university environment is characterized by a high degree of openness, technological interconnectedness, and social dynamism, which naturally increases its vulnerability to physical, cyber, and psychosocial threats. Security therefore cannot be understood as an isolated technical or administrative function, but rather as a comprehensive governance system that links infrastructure, human resources, information technologies, and organizational processes.

An analysis of the literature and available empirical evidence shows that the effective protection of higher education institutions depends on the ability to integrate multiple layers of security within a unified governance framework. The physical protection of campuses, the cybersecurity of information systems, and the psychosocial well-being of students and staff are closely interconnected and mutually reinforcing. For example, digital incidents can lead to a loss of trust and heightened stress within the academic community, while prolonged psychosocial strain can reduce attentiveness, discipline, and the capacity to comply with security procedures. An integrated model therefore enables not only more precise risk identification, but also a deeper understanding of their cumulative and indirect effects.

An important finding also concerns the role of organizational and human factors. Without clearly defined responsibilities, functional crisis plans, and regular training, even technologically advanced security systems remain underutilized or ineffective. Higher education institutions should therefore invest systematically in the development of a security culture that includes not only the professional preparation of crisis teams, but also the awareness of students and staff regarding risks, appropriate procedures, and their own responsibilities. Such an approach strengthens institutional resilience and reduces the likelihood that incidents will escalate into crisis situations.

A major advantage of the integrated framework lies in its support for data-driven decision-making. By linking information on physical incidents, cyber threats, and psychosocial indicators, institutions can develop comprehensive risk profiles that enable preventive

measures to be targeted where they are most needed. This shift from reactive to proactive security management is crucial for modern universities, which face a rapidly evolving threat landscape while also needing to preserve openness, academic freedom, and support for innovation.

Although this study does not present primary empirical data, it provides a structured and integrative analytical framework that connects regulatory requirements, institutional practice and multi-domain risk management in higher education. The strength of the contribution lies in the systematic synthesis of fragmented security perspectives into a coherent governance model supported by operational tools (risk typology, RACI matrix and scenario-based illustration). Future empirical studies can build on this framework to test its effectiveness in specific institutional contexts, but the present work already offers a robust conceptual and practical foundation for university security planning and governance. Taken together, the study provides structured answers to RQ1–RQ4 by defining the key security domains, mapping cross-domain risks and vulnerabilities, examining existing preventive and organizational measures, and synthesizing these insights into an integrated governance framework for higher education security.

Author Contributions: Each author (M.B., I.B., G.W., M.K. and M.H.) equally contributed to this publication. Conceptualization, M.B. and I.B.; methodology, M.B.; software, I.B.; validation, G.W., M.K. and I.B.; formal analysis, G.W. and M.H.; investigation, M.K.; resources, M.B.; data curation, I.B. and G.W.; writing—original draft preparation, M.B. and I.B.; writing—review and editing, I.B. and M.K.; visualization, I.B. and M.H.; supervision, M.B.; project administration, I.B. and G.W.; funding acquisition, I.B. and G.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Scientific Grant Agency of the Ministry of Education, Science, Research, and Sport of the Slovak Republic and the Slovak Academy Sciences as part of the research project VEGA: 1/0039/24, “Research on the Rock Drilling Process through Monitoring of Acoustic and Vibration Signals to Enhance the Efficiency of Mineral Resource Extraction”, and by the “TUKÉ-OU Young Researchers’ Grant” Program.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available in public repositories (Scopus, Web of Science) and in publicly available legislative and institutional documents. These data were derived from the following resources available in the public domain: [e.g., Scopus, Web of Science, national legislation registers, anonymized institutional documents]. Further inquiries can be directed to the corresponding author.

Acknowledgments: The authors would like to thank the anonymous referees for their valuable comments that improved the quality of the manuscript.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Laz-Figueroa, K.; Guevara-Viejó, F.; Valenzuela-Cobos, J.D.; Hernández-Sánchez, B.R.; Sánchez-García, J.C. Gender-Based Violence in Higher Education Institutions in Ecuador: A Systematic Literature Review. *Front. Educ.* **2025**, *10*, 1702277. [[CrossRef](#)]
2. Moylan, C.A.; Nason, J.A. Campus Climate Factors Associated with the Likelihood of Experiencing Sexual Assault in College. *J. Am. Coll. Health* **2025**, 1–9. [[CrossRef](#)]
3. Papp, L.J.; Baker, M.R.; Ward, L.M.; Reed, L.A. Development and Validation of the Acceptance of Sexualized Aggression Scale Among U.S. College Women. *J. Sex Res.* **2025**, 1–17. [[CrossRef](#)] [[PubMed](#)]
4. Sutton, H. AI Weapon Detection: What Campus Safety Officers Need to Know. *Campus Secur. Rep.* **2026**, *22*, 6–13. [[CrossRef](#)]
5. Enelichi, M.; Munonye, C.C.; Udomiaye, E. Students’ Awareness of Fire Safety Measures in a University Building: A Case Study of a Clinical Hostel. *IPS J. Eng. Technol.* **2026**, *2*, 203–208. [[CrossRef](#)]

6. ICDESS. Data and Information Security Analysis in Risk Management Using OCTAVE-S Framework and ISO 27001:2022. *Proc. Int. Conf. Digit. Educ. Soc. Sci.* **2025**, *3*, 51–58. [CrossRef]
7. Dahiru, S.; Musa, A. Use of Biometric Technology for Information Access Control among Undergraduates of Northwest University, Kano. *Libr. Inf. Perspect. Res.* **2025**, *7*, 22–31. [CrossRef]
8. Martinez-Fierro, M.L.; Avila-Carrasco, L.; Basconcelos-Sanchez, J.M.; Peralta-Trejo, I.; Ortiz-Castro, Y.; Luna-Morales, M.E.; Ramirez-Hernandez, L.A.; Martinez-Vazquez, M.C.; Mentali Mental Health Collaborative Network; Garza-Veloz, I. Bullying and Harassment in a University Context: Impact on the Mental Health of Medical Students. *Psychiatry Int.* **2026**, *7*, 8. [CrossRef]
9. Ganson, K.T.; O'Connor, J.; Nagata, J.M. Physical Violence Perpetration Among College Students: Prevalence and Associations With Substance Use and Mental Health Symptoms. *J. Interpers. Violence* **2021**, *37*, NP11110–NP11134. [CrossRef] [PubMed]
10. Haque, M.A.; Ahmad, S.; John, A.; Mishra, K.; Mishra, B.K.; Kumar, K.; Nazeer, J. Cybersecurity in Universities: An Evaluation Model. *SN Comput. Sci.* **2023**, *4*, 569. [CrossRef]
11. Goniewicz, K. Public Health Response to Disasters and Crises: Setting the Agenda for Effective Action. *Int. J. Emerg. Med.* **2025**, *18*, 132. [CrossRef]
12. Hyseni Duraku, Z.; Davis, H.; Arënliu, A.; Uka, F.; Behluli, V. Overcoming Mental Health Challenges in Higher Education: A Narrative Review. *Front. Psychol.* **2024**, *15*, 1466060. [CrossRef]
13. European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2023*; ENISA: Athens, Greece, 2023. Available online: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf> (accessed on 28 February 2026).
14. European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2024: July 2023 to June 2024*; ENISA: Athens, Greece, 2024. Available online: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf (accessed on 28 February 2026).
15. Bwiino, K.; Kituyi Mayoka, G.; Nkamwesiga, L.; Nyamadi, M.; Musenze, I.A. Information Security Behavior in Higher Education Institutions: A Systematic Literature Review. *J. Inf. Secur. Cybercrimes Res.* **2025**, *8*, 43–62. [CrossRef]
16. Afolalu, O.; Tsoeu, M.S. Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions. *Future Internet* **2025**, *17*, 575. [CrossRef]
17. Lallie, H.S.; Thompson, A.; Titis, E.; Stephens, P. Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector. *Computers* **2025**, *14*, 49. [CrossRef]
18. Dolliver, D.S.; Ghazi-Tehrani, A.K.; Poorman, K.T. Building a Robust Cyberthreat Profile for Institutions of Higher Education: An Empirical Analysis of External Cyberattacks against a Large University's Computer Network. *Int. J. Law Crime Justice* **2021**, *66*, 100484. [CrossRef]
19. Leeder, C. How College Students Evaluate and Share “Fake News” Stories. *Libr. Inf. Sci. Res.* **2019**, *41*, 100967. [CrossRef]
20. Rifat, S.I. Spreading of Fake News Among the Students of Jahangirnagar University: Origin, Sharing and Consequences. Master's Thesis, Jahangirnagar University, Savar, Bangladesh, 2026. [CrossRef]
21. Cagle, S.M.; Anderson, A.A.; Kelp, N.C. Stop the Spread: Empowering Students to Address Misinformation through Community-Engaged, Interdisciplinary Science Communication Training. *J. Res. Sci. Teach.* **2024**, *4*, 569. [CrossRef]
22. Mulyani, S.; Gaffar, M.F.; Komariah, A.; Suryadi; Suhendar, A.; Rusnati, I.; Wulansari, S. Academic Management System Integration of Private Universities. *Int. J. Sci. Technol. Manag.* **2021**, *2*, 1095–1101. [CrossRef]
23. Lambovska, M.; Angelova-Stanimirova, A. Unveiling Challenges to Management Control Systems in Higher Education: A Systematic Literature Review. *World* **2025**, *6*, 100. [CrossRef]
24. Raza, K.; Roach, P.; Hardcastle, L.; Hayden, A.; Gereluk, D.; Bharwani, A. A Systematic Review of the Conceptualization, Interpretation, and Implementation of Shared Governance in Post-Secondary Contexts. *Stud. High. Educ.* **2025**, *50*, 1591–1609. [CrossRef]
25. Marquez-Tejon, J.; Jimenez-Partearroyo, M.; Benito-Osorio, D. Integrated security management model: A proposal applied to organisational resilience. *Secur. J.* **2023**, *37*, 375–398. [CrossRef]
26. Klasa, K.; Trump, B.D.; Dulin, S.; Smith, M.; Jarman, H.; Linkov, I. A Resilience-Augmented Approach to Compound Threats and Risk Governance: A Systems Perspective on Navigating Complex Crises. *Environments* **2025**, *12*, 64. [CrossRef]
27. Shen, Q.; Injoungjirakit, N.; Teekasap, S.; Sridama, P. Adoption of Campus IoT in Shanghai Higher Education: A Mixed-Methods UTAUT Study with Infrastructure and Privacy Extensions. *Environ. Soc. Psychol.* **2026**, *11*, ESP-4347. [CrossRef]
28. Wang, W. Exploration of a Psychological Crisis Prevention and Intervention Mechanism in Universities: An Integrated Approach Based on the “Collaborative Assessment and Management of Suicidality” (CAMS) Framework. *J. Educ. Educ. Res.* **2026**, *17*, 24–27. [CrossRef]
29. Parker, L.; Loper, A.J.; Hayes, J.; White, S.; Hallman, H.; Karakas, A. Comparative Analysis of Artificial Intelligence Policies in Universities across Five Countries. *Discov. Comput.* **2025**, *28*, 267. [CrossRef]
30. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Off.*

- J. Eur. Union* **2016**. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (accessed on 28 February 2026).
31. Marín, M.E.A.; Alcantar, J.I.A.; Marcial, M.C.; Franco, E.G.C. Innovation in Biometric Security and Digital Transformation: Redesigning Security Models in Society. *Int. J. Comb. Optim. Probl. Inform.* **2026**, *17*, 166–181. [\[CrossRef\]](#)
 32. Vilorio, Z.P.; Moyao, W.G. Assessment of Emergency Awareness and Preparedness among Students and Employees at Benguet State University—Buguias Campus. *Tech. Soc. Sci. J.* **2026**, *79*, 318–341. [\[CrossRef\]](#)
 33. Zheng, Y.; Vedula, S.; Olajube, A.; Anubi, O. Generative Vulnerability Assessment for Cyber-Physical Systems. *ACM Trans. Cyber-Phys. Syst.* **2026**, *10*, 1–27. [\[CrossRef\]](#)
 34. Kavitha, L.; Shaik, K. The Statistical Analytical Review of IoT Threat Detection Mechanisms: Quantitative Evaluation and Multidimensional Performance Assessment Analysis. *EAI Endorsed Trans. Internet Things* **2026**, *24*, e10529. [\[CrossRef\]](#)
 35. Boustani, N.M.; Mourtaji, L.; Arts-Chiss, N. Learning to Adapt: Educational Technologies and the Construction of Sustainable and Resilient Learning Environments. *Front. Educ.* **2026**, *10*, 1686368. [\[CrossRef\]](#)
 36. Camonias, R.L. Preparedness Level of Christian Polytechnic Institute of Catanduanes (CPIC) in Typhoon and Calamities in the Province of Catanduanes: Baseline for Curriculum Integration. *JPAIR Multidiscip. Res.* **2026**, *63*, 205–222. [\[CrossRef\]](#)
 37. Msheik, A.; Peralta, R.; Al Mokdad, Z.; Bartulec, C.; Abou-Abbas, L.; Anani, D.; Al Mawla, H.; Salame, H.; Moussa, M.; Bahattab, A. Disaster Medicine Training for Medical Students in Lebanon: Quasi-Experimental Comparison of e-Learning and Face-to-Face Modalities. *JMIR Med. Educ.* **2026**, *12*, e80409. [\[CrossRef\]](#)
 38. Mahmood, R.; Ahmed, W.; Mahmood, S.; Suleman, R.M.F.; Shabbir, M.; Wang, F.Y. From Challenges to Coping Strategies. *J. Int. Stud.* **2026**, *16*, 35–62. [\[CrossRef\]](#)
 39. Ouyang, H.; Xie, H.; Wang, Y.; Chen, X.; Cheng, Q.; Hou, B.; Zhang, P. Academic Stress, Cognitive Appraisal, Academic Self-Efficacy, and Academic Anxiety among Chinese College Students: A Moderated Mediation Model. *Acta Psychol.* **2026**, *263*, 106322. [\[CrossRef\]](#)
 40. Wang, Y.; Xu, S. Relationship between Artificial Intelligence Tool Usage Experience and Academic Stress among College Students: Mediating Role of Loneliness and Moderating Role of Academic Self-Efficacy. *Acta Psychol.* **2026**, *263*, 106220. [\[CrossRef\]](#)
 41. Putri, R.U.; Suhadianto; Noviekayati, I. Challenges of Academic Adjustment of First-Year College Students: A Systematic Review of Causative Factors and Consequences. *Int. J. Res. Innov. Soc. Sci.* **2026**, *9*, 905–914. [\[CrossRef\]](#)
 42. Abulfaraj, G.G.; Upsher, R.; Zavos, H.M.S.; Domett, E.J. The Impact of Resilience Interventions on University Students' Mental Health and Well-Being: A Systematic Review. *Educ. Sci.* **2024**, *14*, 510. [\[CrossRef\]](#)
 43. Marcedula, F.; Angelini, G.; Fiorilli, C. Teacher Self-Efficacy and Well-Being: The Mediating Role of Satisfaction with Students, Colleagues, and Parents. *Int. J. Environ. Res. Public Health* **2026**, *23*, 150. [\[CrossRef\]](#) [\[PubMed\]](#)
 44. Cuares, A.; Casaña, K.G. Digital Responsibility of Public Administration Students: Challenges and Coping Strategies. *J. Interdiscip. Perspect.* **2026**, *4*, 227–234. [\[CrossRef\]](#)
 45. Juhaini, J.; Sumiati, S.; Juhari, J. Student Strategies in Maintaining a Balance between Academic Work, Organizational Activities, and Personal Life. *TechTalent Bus. Rev.* **2026**, *1*, 26–37. [\[CrossRef\]](#)
 46. Cotha, K.S.; Jena, A. Insurance Inclusivity in Education: A Conceptual Framework for Student Well-Being, Security, and Access. *Int. Indian Law Rev.* **2026**, *34*, 182–194. [\[CrossRef\]](#)
 47. AlHyasat, O.; Falahat, M. Enhancing University Performance through Cybersecurity Strategy: Evidence from Jordanian Higher Education Institutions. *Cogent Bus. Manag.* **2026**, *13*, 2607812. [\[CrossRef\]](#)
 48. Arduin, P.-E.; Costé, B. Learning to Hack, Playing to Learn: Gamification in Cybersecurity Courses. *J. Cybersec. Priv.* **2026**, *6*, 16. [\[CrossRef\]](#)
 49. Sharko, A.D.; Puravelli, F.; Sharko, G. Strengthening Digital Defense: The Role of Cyber Vaccination and Awareness Training in Modern Cybersecurity Education. *Eur. J. Econ. Law Soc. Sci.* **2026**, *10*, 23–32. [\[CrossRef\]](#)
 50. Bwiino, K.; Mayoka, G.K.; Nkamwesiga, L.; Nyamadi, M. A Systematic Literature Review of Information Security Practices in Higher Education Institutions. *IET Inf. Secur.* **2026**, *2026*, 6324508. [\[CrossRef\]](#)
 51. Kularski, C.M.; Martin, F. Online Student Privacy in Higher Education: A Systematic Review of the Research. *Am. J. Distance Educ.* **2022**, *36*, 227–241. [\[CrossRef\]](#)
 52. Almugamisi, H. Emotional Perceptions of Data Breaches as Diagnostic Indicators of Data Governance Maturity in Saudi Higher Education. *Discov. Psychol.* **2026**, *6*, 48. [\[CrossRef\]](#)
 53. Ngoc, L.B. Artificial Intelligence in Personalized Learning and Student Assessment: Challenges and Implementation Solutions. *J. Manag. Res. Rev.* **2026**, *2*, 1–6. [\[CrossRef\]](#)
 54. Mollaki, V.; Ziouvelou, X.; Giouvanopoulou, K.; Karkaletsis, V. Challenges and Recommendations for Research Security: Learning from Research Ethics and Integrity. *Res. Ethics* **2026**, *2026*, 17470161251404962. [\[CrossRef\]](#)
 55. Shih, Y.-H. The Transformation of Higher Education in the Context of Globalization: Implications from Paulo Freire's Critical Pedagogy. *Front. Educ.* **2026**, *10*, 1714343. [\[CrossRef\]](#)

56. Mtaka, H. Integrated Risk Management Approaches for Enhanced Project Performance in Higher Education Institutions: A Tanzanian Perspective. *Int. J. Multidiscip. Res. Growth Eval.* **2026**, *7*, 495–499. [[CrossRef](#)]
57. Damarched, M.K. Digital Transformation Strategies for Higher Education—Enterprise IT Systems. *Int. J. Nov. Res. Dev.* **2026**, *11*, b780–b791. [[CrossRef](#)]
58. Okulicz-Kozaryn, W.; Artyukhov, A.; Artyukhova, N. Will AI Replace Us? Changing the University Teacher Role. *Societies* **2026**, *16*, 32. [[CrossRef](#)]
59. Purwaamijaya, B.M.; Prasetyo, Y.; Nidar, S.R.; Nazya, A.F. Achievement of SDGs through the Role of Artificial Intelligence in Human Resources from a Gen-Z Perspective. *J. EMT KITA* **2026**, *10*, 228–235. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.