ASSESSMENT AND MANAGEMENT OF TECHNOLOGICAL RISKS IN THE DIGITALIZATION PROCESS OF ACADEMIC INSTITUTIONS

Ivona Velkova[1],
e-mail: ivonavelkova@unwe.bg [1],

Абстракт

Дигитализацията в академичните институции предоставя възможности за по-голяма ефективност, подобрена достъпност и оптимизирано управление на образователните процеси. В същото време тя поражда редица технологични рискове, които могат да възпрепятстват институционалните дейности, да компрометират сигурността на данните и да нарушат непрекъснатостта на учебния и научноизследователския процес. Настоящото изследване представя систематичен обзор на основните технологични рискове в академичната среда, включително нарушения на сигурността и поверителността на данните, системни откази и прекъсвания на услуги, както и остаряване на технологиите. Предлага се методологична рамка за идентифициране, оценка и приоритизиране на тези рискове чрез използване на матрица „вероятност – въздействие - готовност“. Примери от университетската практика и международни стандарти (ENISA, NCSC, ISO 27001, GDPR) се използват за илюстриране на често срещани уязвимости и подходи за управление. Анализът подчертава повтарящи се модели като висока зависимост от външни доставчици, недостатъчна готовност за възстановяване при бедствия и рискове, свързани с остарели технологии. Резултатите акцентират върху необходимостта от систематична оценка и приоритизация на рисковете, което ще позволи на академичните институции да укрепят своята устойчивост и да осигурят сигурна и ефективна дигитализация.

Abstract

Digitalization in academic institutions provides opportunities for greater efficiency, improved accessibility, and optimized management of educational processes. At the same time, it generates a range of technological risks that may hinder institutional operations, compromise data security, and disrupt the continuity of teaching and research activities. This study presents a systematic overview of the main technological risks in the academic environment, including data security and privacy breaches, system failures and service interruptions, as well as technology obsolescence. A methodological framework is proposed for the identification, assessment, and prioritization of these risks through the use of a likelihood - impact - readiness matrix. Examples from university practice and international standards (ENISA, NCSC, ISO 27001, GDPR) are included to illustrate common vulnerabilities and management approaches. The analysis highlights recurring patterns such as high dependency on external providers, insufficient disaster recovery preparedness, and risks associated with outdated technologies. The results emphasize the need for systematic risk assessment and prioritization, enabling academic institutions to strengthen their resilience and support secure and effective digitalization.

Keywords: digitalization, technological risks, cybersecurity, academic institutions

JEL: I2, I23, I24, O33

Introduction

Digitalization has become one of the driving forces behind the transformation of higher education. Universities depend on digital systems in almost every area of their activity, from administration and teaching support to virtual classrooms and research management. Thanks to this shift, universities have gained broader access to information and more agile ways of working, while cooperation between

[1] Гл. ас. д-р в катедра ИТК, УНСС, e-mail: ivonavelkova@unwe.bg

disciplines and regions has become smoother and more natural. Still, the growing dependence on technology also carries new risks. System failures, data breaches, or poorly secured platforms can quickly disrupt academic life, threaten the continuity of education, and erode institutional trust and reputation [1].

At the core of this digital transformation are the technologies that keep academic life running - hardware and software, learning management systems (LMS), student information systems (SIS), research databases, cloud services, and a growing range of digital tools. These systems make modern universities possible, yet they also come with their own risks. Cyberattacks, system failures, outdated components, or poor integration can all interrupt daily operations and expose critical data [2].

The challenge has grown as new digital tools continue to appear, each requiring fresh investment, training, and technical adaptation. The links between systems make things even more complicated. When an LMS platform connects with identity management or national research networks, a single weak point can trigger a chain reaction across multiple services [3]. Many universities also face another constraint - limited funding and a shortage of skilled IT professionals - which makes it harder to maintain strong security and lasting technological resilience [2].

In recent years, cybersecurity agencies such as ENISA have pointed out that higher education remains one of the sectors most at risk. Large data breaches, ransomware incidents, and system outages during online exams have shown how quickly technical problems can escalate - from temporary disruptions to serious breaches of trust between institutions, students, and staff [4].

That’s why a systematic look at technological risks in academia is so important. Understanding these challenges means not only identifying specific threats but also seeing how they connect. For instance, an outdated system may cause compatibility problems that make a network more vulnerable to attack. A comprehensive analysis should therefore bring together theory, real-world cases, and cross-institutional comparisons to reveal these relationships.

This paper focuses on how technological risks in higher education can be assessed and managed more effectively. It aims to outline the key risk factors, explain their causes and effects, and point to practical ways to address them. Using examples from university experience and established frameworks such as the GDPR, ISO/IEC 27001, and the NIST Cybersecurity Framework, the study links conceptual understanding with hands-on strategies for building stronger digital resilience in higher education.

Methodology

The paper adopts a structured and systematic methodology to identify, assess, and prioritize technological risks in the digitalization of higher education. The analysis focuses on the technological dimension of institutional risk, deliberately excluding organizational, financial, and human factors to maintain methodological precision. It follows an exploratory–descriptive design that combines qualitative analysis of secondary data such as incident reports, institutional policies, and international frameworks - with an analytical model classifying risks by frequency, impact, and institutional readiness. The resulting framework bridges conceptual understanding with practical evaluation and reflects the realities of digital transformation across academia.

The methodology draws on several internationally recognized sources, including the ENISA Threat Landscape 2023 [4], the EDUCAUSE Horizon Report 2022 [5], ISO/IEC 27001 [6], the NIST Cybersecurity Framework [7], and the principles of the General Data Protection Regulation (GDPR) [8]. These standards and reports were selected because they provide widely accepted criteria for understanding and managing technological risks in the public and educational sectors. They also ensure consistency and comparability with existing research and policy practices.

Risk Matrix Construction and Data Sources

To assess the technological risks affecting academic institutions, this study employed a likelihood - impact - readiness matrix as a core analytical tool. The matrix was designed to synthesize information from multiple qualitative and quantitative sources, enabling a balanced and transparent evaluation of risk exposure.

1. Data Sources

The construction of the matrix relied on three primary sources of evidence:

- International threat intelligence and sector reports – including ENISA Threat Landscape for Education 2023 [4], EDUCAUSE Horizon Report 2022 [5], and Jisc Cybersecurity Posture of UK Higher Education 2022 [9], which provided sector-wide statistics on incident frequency, attack types, and recurring vulnerabilities.
- Documented university case studies – such as the University of Manchester data breach (2023) [10], the University of Waterloo ransomware attack (2023) [11], and the cybersecurity incident at Mount Saint Mary College in 2022 [12]. These examples provide concrete evidence of how cybersecurity incidents in higher education can affect institutions financially, operationally, and reputationally.
- Regulatory and technical standards – namely ISO/IEC 27005 (Information Security Risk Management) [6], ISO 31000 (Risk Management Guidelines) [13], and NIST SP 800-30 (Guide for Conducting Risk Assessments) [14]. These frameworks provided the conceptual foundation for defining scales and evaluation criteria.

2. Evaluation Logic

Each risk category was assessed along three dimensions:

- Likelihood: determined from the frequency and recurrence of incidents reported in ENISA, EDUCAUSE, and Jisc data. Risks appearing in two or more independent sources were rated High; those mentioned sporadically were Medium; and isolated or hypothetical risks were Low.
- Impact: assessed using case study evidence on the extent of service disruption, cost of recovery, data loss magnitude, and reputational damage. Severe multi-system or regulatory consequences (GDPR fines) were rated Critical; moderate single-system disruptions High; and limited local effects Medium.
- Readiness: evaluated through the presence of preventive and response measures observed in university audits and policy documents (MFA enforcement, backup testing frequency, DPO appointment). Institutions exhibiting multiple active controls were considered High readiness; minimal or reactive measures Low.

3. Integration and Scoring

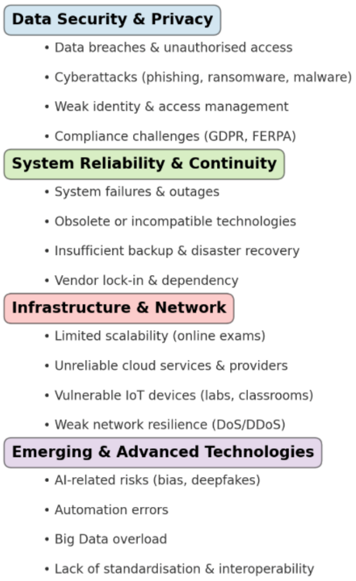
The three dimensions were combined using a qualitative matrix model, where risk priority equals the combined weight of likelihood and impact, adjusted by readiness. For instance, a High-likelihood and High-impact risk with Low readiness was classified as Critical, while the same risk with High readiness was downgraded to High. This weighting ensures that strong institutional preparedness can mitigate otherwise severe risks.

4. Validation

The resulting matrix was informed by international benchmarks published by ENISA and EDUCAUSE to maintain consistency with sector-level perspectives. While the assessment remains qualitative, drawing on multiple data sources supports its reliability and comparability across institutions.

The process of identifying risks began with an analytical review of documented cybersecurity incidents and sector reports related to higher education. Common patterns were derived from international analyses and institutional experiences described in publicly available sources. Each identified risk was then examined according to its technological characteristics and its relevance to the academic environment. From this analysis, four major categories were defined: data security and privacy, system reliability and continuity, infrastructure and network, and emerging and advanced technologies. These categories represent the main technological domains of higher education most frequently exposed to disruption. Selected institutional incidents, referenced in the accompanying matrix, illustrate how these risk categories manifest in practice across different universities.

The classification of these risk domains represents the author’s analytical synthesis, developed by comparing existing frameworks and academic sources. While ENISA, EDUCAUSE, and ISO/IEC 27001 outline various typologies of digital risk, this study integrates their principles into a unified model tailored to the context of higher education. This combined approach allows for a focused assessment of the technological dimension of risk while maintaining consistency with internationally recognized standards.


Data Security & Privacy
• Data breaches & unauthorised access
• Cyberattacks (phishing, ransomware, malware)
• Weak identity & access management
• Compliance challenges (GDPR, FERPA)
System Reliability & Continuity
• System failures & outages
• Obsolete or incompatible technologies
• Insufficient backup & disaster recovery
• Vendor lock-in & dependency
Infrastructure & Network
• Limited scalability (online exams)
• Unreliable cloud services & providers
• Vulnerable IoT devices (labs, classrooms)
• Weak network resilience (DoS/DDoS)
Emerging & Advanced Technologies
• AI-related risks (bias, deepfakes)
• Automation errors
• Big Data overload
• Lack of standardisation & interoperability

Source:Author’s research

Figure 1. Classification of technological risks in Academia

Figure 1 gives an overview of how technological risks in higher education are grouped into four main areas. It also provides the basis for the next section, which explores each category through its key causes, resulting impacts, and ways these risks can be mitigated.

To evaluate and prioritize the identified risks, the analysis employs the previously described matrix. This framework consolidates the findings from the data review and enables a structured comparison across risk categories. By visualizing the combined dimensions of frequency, potential impact, and institutional preparedness, the matrix indicates which risks may warrant immediate strategic attention and which are more suitable for gradual capacity development. The resulting assessment provides the basis for the comparative and analytical discussion in the following sections.

Finally, the analysis compares findings from various universities and international studies to identify recurring challenges and interdependencies. The comparison reveals patterns such as strong dependence on external service providers, outdated technologies, and limited investment in disaster recovery. These insights form the foundation for the subsequent sections, which examine each risk category in greater detail and propose strategies for strengthening technological resilience in higher education.

Analysis of technological risks in Academia

The digital transformation of higher education has reshaped the way universities function, integrating teaching, research, and administration into a single interconnected digital ecosystem. While this transformation enables innovation and operational efficiency, it also introduces new layers of technological risk that can compromise data integrity, interrupt academic services, and undermine institutional reputation. According to recent international analyses of cybersecurity in higher education, the sector remains among the most frequently targeted by cyber threats due to the high value of academic data, the decentralization of IT infrastructures, and often constrained cybersecurity budgets.

Building on the methodological framework presented earlier, this section examines four main categories of technological risks that define the academic digital landscape: data security and privacy, system reliability and continuity, infrastructure and network, and emerging and advanced technologies.

Data security and privacy

Universities manage vast repositories of sensitive data - including student information, research outputs, and administrative records - making them attractive targets for cyberattacks. Data security and privacy violations are the most critical category of technological risk, given their potential to disrupt operations, violate regulations such as the GDPR, and erode institutional trust.

Table 1. Key indicators and evaluation of data security and privacy risks

Subcategory	Key Indicators	Likelihood	Impact	Priority
Data breaches and unauthorized access	Number of incidents per year; time to detect and recover; volume of exposed records	High	Critical	Critical
Cyberattacks (phishing, ransomware, malware)	Frequency of attacks; downtime duration; recovery cost	High	High	High
Weak identity & access management (IAM)	MFA adoption; inactive accounts; privilege misuse	Medium-High	High	High
Compliance challenges (GDPR, ISO/FERPA)	Number of data protection incidents; regulator notifications; vendor compliance rate	Medium	Medium-High	Moderate-High

Source: Author's synthesis based on multiple international frameworks and reports (ENISA, EDUCAUSE, NIST, ISO 27001, GDPR)

Data security breaches and ransomware attacks represent the most severe risks for academic institutions. Their likelihood is consistently high due to the openness of academic networks and the diversity of users, while the impact includes service disruption, reputational loss, and legal penalties. Weak identity management and fragmented compliance practices further increase exposure.

Effective mitigation requires a layered defense model combining technical controls (encryption, MFA), organizational measures (Data Protection Officer, incident response planning), and cultural interventions (awareness training). Integrating these measures under GDPR, ISO/IEC 27001, and the NIST Cybersecurity Framework significantly enhances institutional readiness.

System reliability and continuity

Academic operations depend on the continuous availability of digital systems supporting teaching, research, and administration. Failures in this area—caused by aging infrastructure, insufficient redundancy, or vendor dependency—can lead to widespread disruption. Table 2 outlines the main subcategories of system reliability risks, together with key indicators, likelihood, and relative priority, as identified in the analytical framework.

Table 2. System reliability and continuity risks

Subcategory	**Key Indicators**	**Likelihood**	**Impact**	**Priority**
System failures and outages	Number of critical service interruptions; uptime percentage	High	High	Critical
Obsolete or incompatible technologies	% of unsupported systems; integration failures	Medium-High	High	High
Insufficient backup and recovery	Backup frequency; test success rate; RPO/RTO metrics	Medium	High	High
Vendor dependency	% of outsourced critical services; strength of SLAs	Medium	Medium–High	Moderate-High

Source: Author's synthesis based on multiple international frameworks and reports (ENISA, EDUCAUSE, NIST, ISO 27001, GDPR)

In higher education, system reliability risks often surface only during major service disruptions. Evidence from institutional reports indicates that limited recovery testing and outdated technologies exacerbate the duration and cost of outages. To address these vulnerabilities, institutions should adopt redundant architectures, conduct structured recovery exercises, and align continuity objectives (RTO/RPO) with established standards such as ISO 27031 and ITIL Service Operations.

Infrastructure and network

The backbone of digital academia lies in its infrastructure: cloud platforms, network systems, IoT devices, and scalable connectivity. While these components enable efficiency and flexibility, they also introduce new vulnerabilities.

Table 3. Indicators and assessment of infrastructure & network risks

Subcategory	**Key Indicators**	**Likelihood**	**Impact**	**Priority**
Limited scalability (online exams)	Maximum concurrent capacity; response time under stress	High	High	Critical
Unreliable cloud services and providers	Frequency of outages; provider diversification	Medium-High	High	High
Vulnerable IoT devices	Unauthenticated devices; detected vulnerabilities	Medium	Medium-High	Moderate-High
Weak network resilience (DoS/DDoS)	Number of incidents per year; mitigation capability	High	Medium-High	High

Source: Author's synthesis based on international cybersecurity and infrastructure resilience frameworks (ENISA Cloud Security Guidelines, NIST Cybersecurity Framework, ISO/IEC 27036).

Infrastructure failures - especially during online examinations or registration peaks - have direct academic and operational consequences. Cloud dependency and the growing number of IoT devices expand the attack surface, while DDoS attacks remain among the most frequent disruptions.

Mitigation requires proactive capacity planning, multi-cloud diversification, IoT segmentation, and network redundancy. Documented incidents in higher education demonstrate that insufficient scalability or insecure endpoints can rapidly escalate into institution-wide service failures. International standards such as ISO/IEC 27036, the ENISA Cloud Security Guidelines, and the NIST Cybersecurity Framework offer structured guidance for strengthening technological resilience.

Emerging and advanced technologies

The rapid deployment of AI, automation, and big data systems in academia offers significant opportunities for innovation but also introduces new categories of technological risk. AI-driven integrity challenges, automation errors in assessment platforms, and inadequate data governance can undermine institutional integrity and operational efficiency.

Table 4. Indicators and assessment of emerging technology risks

Subcategory	Key Indicators	Likelihood	Impact	Priority
AI-related misuse	% of flagged submissions; integrity violations	High	High	Critical
Automation errors	Number of process failures; manual intervention rate	Medium-High	High	High
Big data overload	Data utilization rate; storage-to-processing ratio	Medium	Medium-High	Moderate-High
Lack of interoperability	Integration failures; % of systems using open standards	Medium	High	High

Source: Author’s synthesis based on principles from the UNESCO Recommendation on the Ethics of AI (2021) [15]*, the EU AI Act (draft, 2024)* [16]*, and ISO/IEC 38505 (Data Governance)* [17].

The integration of emerging technologies in higher education introduces both opportunities and vulnerabilities. Institutions face growing challenges related to AI-driven academic integrity, automation reliability, and the governance of large and complex datasets. In many cases, these risks stem from rapid adoption without adequate oversight, ethical frameworks, or interoperability standards.

Effective mitigation requires a balanced approach that combines innovation with governance: establishing AI ethics policies, ensuring human oversight in automated processes, and implementing strong data lifecycle management practices.

Comparative evaluation and discussion

Looking across all four domains, it becomes clear that technological risks in academia rarely act in isolation. System failure can expose data vulnerabilities, while inadequate governance over emerging technologies can intensify both security and reliability concerns. These patterns show that universities face a web of interconnected risks rather than discrete problems. Table 5 summarizes this relationship by comparing likelihood, impact, and priority across each category.

Table 5. Consolidated comparative risk matrix for academic institutions

Risk Category	Likelihood	Impact	Priority	Justification
Data Security and Privacy (breaches, cyberattacks, IAM, compliance)	High	Critical	Critical	Real-world incidents, such as the 2023 data breach at the University of Manchester, the ransomware attack at the University of Waterloo (2023), and the cybersecurity incident at Mount Saint Mary College (2022), demonstrate the tangible consequences of cybersecurity failures in higher education. These events often result in GDPR penalties, reputational loss, and disruption of teaching and research, making this the most visible and damaging risk category.
System Reliability and Continuity (outages, backup failures, vendor dependency)	Medium–High	High	High	Failures during exams or enrolment disrupt critical operations. These are often caused by underfunded IT systems, weak continuity planning, and heavy reliance on external service providers.
Infrastructure and Networks (scalability, cloud outages, IoT insecurity, DDoS)	Medium	High	High	Attacks and failures propagate rapidly across interconnected systems. IoT vulnerabilities and cloud dependencies create systemic risks, particularly during high-demand periods.
Emerging and Advanced Technologies (AI misuse, automation errors, data overload, lack of standards)	Medium–High	High	High	Misuse of AI tools is increasingly common, while automation errors and interoperability gaps undermine academic credibility and long-term sustainability. The impact grows as adoption accelerates.

Source: Author’s synthesis based on comparative analysis of institutional risk domains and international cybersecurity frameworks.

Among all categories, Data Security and Privacy remains the most critical due to its high frequency and severe consequences. However, the remaining domains: System Reliability, Infrastructure and Networks, and Emerging Technologies - are closely interconnected. For example, outdated infrastructure can exacerbate data breaches, while weak governance over AI systems can amplify both privacy and integrity risks.

These interconnections highlight the need for a holistic approach to technological risk management - one that integrates cybersecurity, infrastructure resilience, and responsible innovation governance. A reactive response to individual incidents is no longer sufficient. Instead, universities should cultivate institutional digital resilience grounded in prevention, continuous monitoring, and the ability to recover rapidly from technological disruptions.

Recommendations

Strengthening technological resilience in higher education requires a coordinated and long-term strategy that connects governance, infrastructure, and human capacity. Based on the findings of this study, several key directions can guide universities in managing technological risks more effectively.

A first priority is to establish an integrated risk management framework that unites institutional policies, technical standards, and operational practices. Universities should align their internal governance with international models such as ISO 31000, ISO/IEC 27001, and the NIST Cybersecurity Framework. This alignment ensures that risk identification, assessment, and response activities follow a consistent logic across departments and campuses. It also helps transform cybersecurity from a reactive function into a continuous management process.

Equally important is the need to enhance data governance and compliance mechanisms. Academic institutions handle sensitive research outputs and personal information that demand rigorous protection under regulations such as the GDPR. Implementing privacy-by-design principles, conducting periodic audits, and maintaining clear accountability structures are essential steps. Establishing dedicated Data Protection Officers and cross-departmental privacy committees can further embed compliance within the university culture rather than treating it as an external requirement.

A third strategic area involves system reliability and continuity planning. The study revealed that many universities still rely on legacy systems and ad-hoc recovery procedures. Institutions should define measurable recovery time and recovery point objectives (RTO/RPO), test them regularly through simulation exercises, and secure sufficient financial resources for infrastructure renewal. Emphasizing redundancy, automated backups, and cloud failover solutions can minimize downtime and preserve academic operations during crises.

Another crucial step is to invest in scalable and secure infrastructure. As demand for digital services expands, universities must ensure that their network capacity, cloud architecture, and IoT devices can adapt without compromising security. Multi-cloud diversification, continuous network monitoring, and segmentation of connected devices can substantially reduce the impact of targeted attacks and technical failures.

The rapid adoption of artificial intelligence, analytics, and automation also calls for ethical and responsible innovation practices. Universities should develop clear institutional policies on AI use in research and teaching, promote algorithmic transparency, and encourage human oversight in automated decision-making. Embedding AI literacy and digital ethics into academic curricula will help prepare students and staff to navigate emerging technological challenges responsibly.

Beyond technical measures, technological resilience depends on people as much as on systems. Building a security-first organizational culture requires continuous awareness programs, targeted training, and the encouragement of responsible digital behavior among both students and staff. Simulated phishing campaigns, peer-learning workshops, and the recognition of secure practices can gradually transform cybersecurity from individual responsibility into a shared institutional value.

Taken as a whole, these recommendations point toward a more resilient and ethically aware digital future for higher education. Technology in this context should not be viewed only as a set of systems or tools, but as a living part of the institution’s culture and decision-making. When universities see technology as something that connects people, ideas, and responsibilities, they build the capacity not only to respond to crises but also to evolve with them - anticipating change, adapting to it, and emerging stronger each time.

Conclusion

Digital transformation in academia has created both opportunities and vulnerabilities. This paper demonstrates that while digital tools enhance efficiency and access, they also amplify exposure to complex technological risks. The findings confirm that universities face an intertwined network of challenges - where weaknesses in data security, infrastructure, and system reliability can reinforce one another, magnifying institutional exposure.

The likelihood-impact-readiness framework proved effective for mapping these interdependencies and for prioritizing actions according to institutional preparedness. The analysis revealed that the most pressing risks stem from data security and privacy breaches, outdated infrastructure, and the rapid, often unregulated adoption of emerging technologies such as artificial intelligence. These factors together highlight the urgent need for integrated governance mechanisms and continuous monitoring to maintain academic continuity and trust.

Strengthening technological resilience, therefore, requires more than technical upgrades. It calls for strategic alignment between IT, policy, and education; sustainable funding for infrastructure renewal; and the promotion of digital ethics across teaching and research. Universities that embed these principles into their long-term strategies will be better equipped not only to prevent incidents but also to adapt and evolve through future disruptions.

Looking ahead, further research could deepen this model by quantifying risk readiness or comparing maturity levels across national contexts. Such insights would help policymakers and university leaders design more targeted, evidence-based interventions that support secure, inclusive, and sustainable digital transformation in higher education.

Acknowledgement

The paper is prepared as a part of the research activities under the project Models and Instruments for Transforming Higher Education System through Transnational Multi-Sector Links - STUDIES – DIG (Project N: 101131544), funded by the European Union.

References

1. H. Schuetze, W. de Vries, and G. Alvarez Mendiola, “Digitalization of Higher Education,” J. Comp. Int. High. Educ., vol. 16, no. 2, pp. 6–12.
2. В. Андонов, „Софтуерни средства за дигитализиране на основните процеси и услуги във висшите училища на Република България,“ Икономически и социални алтернативи, т. 29, бр. 4, с. 86–94, 2023.

   (Andonov, V., “Software tools for digitalizing the core processes and services in Bulgarian universities,” Economic and Social Alternatives, vol. 29, no. 4, pp. 86–94, 2023.)
3. European Union Agency for Cybersecurity, Identifying Emerging Cybersecurity Threats and Challenges for 2030, LU: Publications Office, 2023. [Online]. Available: https://data.europa.eu/doi/10.2824/117542
4. ENISA, ENISA Threat Landscape 2023. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
5. K. Pelletier, M. McCormack, J. Reeves, J. Robert, and N. Arbino, 2022 EDUCAUSE Horizon Report: Teaching and Learning Edition. EDUCAUSE, Boulder, CO, USA, 2022. [Online]. Available: http://www.educause.edu

6. International Organization for Standardization, ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. [Online]. Available: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en
7. National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, Gaithersburg, MD, NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.
8. European Commission, Principles of the GDPR. [Online]. Available: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/principles-gdpr_en
9. Jisc, Cyber Impact Report 2022. [Online]. Available: https://repository.jisc.ac.uk/8732/1/cyber-impact-report-2022.pdf
10. University of Manchester, “Cyber Incident Statement,” 2023. [Online]. Available: https://www.manchester.ac.uk/about/news/cyber-incident-statement/
11. University of Waterloo, Daily Bulletin – June 6, 2023. [Online]. Available: https://uwaterloo.ca/daily-bulletin/2023-06-06
12. Mount Saint Mary College, “Cybersecurity Incident Statement,” 2022. [Online]. Available: https://www.msmc.edu/newsroom/news/cybersecurity-incident-at-msmc/
13. International Organization for Standardization, ISO 31000:2018 – Risk Management – Guidelines. [Online]. Available: https://www.iso.org/standard/65694.html
14. Joint Task Force Transformation Initiative, Guide for Conducting Risk Assessments, NIST SP 800-30r1, Gaithersburg, MD, USA, 2012. doi: 10.6028/NIST.SP.800-30r1.
15. UNESCO, Recommendation on the Ethics of Artificial Intelligence, 2021. [Online]. Available: https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence
16. European Union, The European Union Artificial Intelligence Act (Draft), 2024. [Online]. Available: https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/public-policy/documents/ey-gl-eu-ai-act-07-2024.pdf
17. International Organization for Standardization, ISO/IEC 38505-1:2017 – Governance of IT – Governance of Data – Part 1: Application of ISO/IEC 38500 to the Governance of Data. [Online]. Available: https://www.iso.org/standard/56639.html