CYBERSECURITY MANAGEMENT MODELS IN HIGHER EDUCATION INSTITUTIONS ACCORDING TO NIS2 REQUIREMENTS

CZU: 378:[005:004.056]
DOI: https://doi.org/10.53486/tids2026.34

KRASIMIR SHISHMANOV
D. A. Tsenov Academy of Economics, Bulgaria
e-mail: k.shishmanov@uni-svishtov.bg
ORCID ID: 0000-0001-9874-2149

YURIY KUZNETSOV
D. A. Tsenov Academy of Economics, Bulgaria
e-mail: y.kuznetsov@uni-svishtov.bg
ORCID ID: 0009-0009-3569-7614

ISKREN TAIROV
D. A. Tsenov Academy of Economics, Bulgaria
e-mail: i.tairov@uni-svishtov.bg
ORCID ID: 0000-0002-2971-5451

Abstract. Higher education institutions (HEIs) are increasingly exposed to cybersecurity threats due to the growing reliance on digital platforms, cloud services, and the handling of sensitive research and personal data. The EU NIS2 Directive establishes a regulatory framework that strengthens cybersecurity obligations, including risk management, incident reporting, policy implementation, and staff awareness. This paper explores internationally recognized cybersecurity management models – ISO/IEC 27001, NIST Cybersecurity Framework, COBIT, and maturity models – and examines their application in higher education settings. A comparative mapping illustrates how these models help HEIs achieve compliance with NIS2 requirements while enhancing their overall cybersecurity posture. The paper also discusses specific challenges, such as limited budgets, technical expertise, and cultural barriers, and provides practical recommendations for gradual and sustainable adoption of cybersecurity practices in universities.

Keywords: cybersecurity, higher education, NIS2, models.

JEL Classification: L86

INTRODUCTION

In the digital era, higher education institutions (HEIs) face increasing cybersecurity threats due to the vast amount of sensitive data they process, including research findings, student records, and intellectual property (Salam *et al.*, 2026). The adoption of robust cybersecurity management models is therefore critical to protect institutional assets and ensure operational continuity. The EU Directive on Security of Network and Information Systems (NIS2) provides a regulatory framework that aims to enhance cybersecurity resilience across member states, including obligations for higher education institutions (European Commission, 2022). This research examines cybersecurity management models applicable to HEIs and evaluates their alignment with NIS2 requirements.

1. Materials and Methods

1.1. Materials

The study focuses on the following materials:

- **NIS2 Directive** – official EU regulatory text and ENISA guidance (European Commission, 2022).
- **Cybersecurity Management Models**:
  - ISO/IEC 27001: Information Security Management System (Calder, 2008)
  - NIST Cybersecurity Framework (NIST, 2018)
  - COBIT 2019 (ISACA, 2021)
  - Cybersecurity Maturity Models (Bada *et al.*, 2019)

These frameworks were selected due to their wide adoption in organizational cybersecurity and compatibility with NIS2 requirements.

1.2 Methods

- A comparative literature review was conducted to analyze how each model addresses NIS2 requirements.
- Mapping of NIS2 obligations to cybersecurity management models was performed, identifying practical strategies for implementation in HEIs.
- Analysis of challenges and recommendations for adoption was derived from case studies and peer-reviewed publications in the field of cybersecurity in higher education (Afolalu and Tsoeu, 2025).

2. Results and Discussion

2.1. Overview of NIS2 Directive

NIS2 is a legislative update to the original NIS Directive, expanding its scope and strengthening security obligations for organizations considered essential or important for societal functions, including universities (European Commission, 2022). Key requirements include:

1. **Risk assessment and management** – Organizations must identify and manage risks to network and information systems.
2. **Incident reporting** – Significant cybersecurity incidents must be reported promptly, typically within 24 hours.
3. **Implementation of security policies** – Organizations must develop internal security policies and incident response plans.
4. **Training and awareness** – Staff must be regularly trained to recognize and respond to cybersecurity threats.

NIS2 emphasizes not only technical measures but also organizational and governance aspects, aligning with global standards for information security.

2.2. Cybersecurity Management Models

Several internationally recognized models can guide HEIs in implementing NIS2-compliant cybersecurity programs:

2.2.1 ISO/IEC 27001

ISO/IEC 27001 defines requirements for an Information Security Management System (ISMS), focusing on continuous risk assessment and mitigation (Kitsios, 2023). It provides a structured approach to information security governance and is widely adopted in educational institutions (Calder, 2008).

2.2.2 NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF), developed in 2014 by the U.S. National Institute of Standards and Technology is based on five functions: Identify, Protect, Detect, Respond, and

Recover (NIST, 2018). Its flexibility makes it suitable for universities with diverse IT infrastructures, integrating technical and administrative controls to manage cyber risks effectively (Riega *et al.,* 2025).

2.2.3 COBIT

COBIT(Control Objectives for Information Technologies) offers a governance and management framework for IT, ensuring alignment with organizational goals and regulatory requirements (ISACA, 2021). Its focus on performance measurement and control is particularly useful for HEIs needing to demonstrate compliance with NIS2.

2.2.4 Maturity Models

Maturity models assess the current state of cybersecurity capabilities and guide incremental improvements. Universities can use these models to benchmark their security posture and align with NIS2's risk-based approach (Papachristofis *et al.,* 2025).

2.3. Application in Higher Education Institutions

Universities face unique cybersecurity challenges, including open network environments, remote learning platforms, and sensitive research data. Applying the aforementioned models helps address these risks:

- **Centralized Security Operations Center (SOC)** – Monitoring and response to cyber incidents in real-time.
- **Regular audits and penetration testing** – Ensuring vulnerabilities are identified and remediated.
- **Policy development and training** – Formal policies and continuous awareness programs for staff and students.

Integration with NIS2 ensures that these practices are not only effective but also compliant, with documented risk assessments, incident response procedures, and reporting mechanisms (Mentzelou *et al.,* 2025).

To provide a clear overview of how higher education institutions can implement NIS2 requirements using various cybersecurity management models, Table 1 maps the main NIS2 obligations to ISO/IEC 27001, NIST CSF, COBIT, and maturity models. This mapping illustrates practical approaches for universities to ensure compliance and strengthen their cybersecurity posture.

Table 1: Mapping NIS2 Requirements to Cybersecurity Management Models in Higher Education Institutions

NIS2 Requirement	ISO/IEC 27001	NIST Cybersecurity Framework	COBIT	Maturity Models	Example Implementation in Universities
Risk Assessment & Management	Risk assessment procedures, controls selection	Identify function: Asset management, risk analysis	Risk management and governance objectives	Evaluate current cybersecurity maturity and gaps	Conduct annual risk assessment of IT systems and research databases
Incident Reporting	Incident management and corrective actions	Respond function: Incident response plans	Monitor and report incidents to management	Track incident response capability in maturity assessment	Establish SOC and formal reporting channels within 24 hours

NIS2 Requirement	ISO/IEC 27001	NIST Cybersecurity Framework	COBIT	Maturity Models	Example Implementation in Universities
Security Policies & Procedures	Information security policies, documentation	Protect function: Access control, awareness training	Define and enforce IT governance policies	Policy maturity evaluation	Develop policies for data protection, cloud use, and remote access
Training & Awareness	Staff awareness programs	Protect & Detect: Awareness, monitoring	Performance metrics for staff compliance	Assess staff training effectiveness	Regular cybersecurity workshops for faculty and students
Continuous Improvement	Internal audits, management reviews	Recover function: Lessons learned, improvements	Measure performance and controls effectiveness	Stage-wise maturity improvement plan	Quarterly review of security controls, update based on audit findings

2.4. Challenges and Recommendations

Higher education institutions face several unique challenges when implementing cybersecurity measures in accordance with NIS2v (Zaid, 2024). One of the primary obstacles is budgetary constraints. Universities often operate with limited financial resources, which can restrict their ability to invest in advanced security technologies, hire specialized cybersecurity personnel, or maintain continuous monitoring systems. This financial limitation makes it difficult to implement comprehensive solutions across all departments and services, potentially leaving some assets more vulnerable than others (Ghulam, 2025).

Another significant challenge is the limited technical expertise among academic and administrative staff. While IT departments may possess skilled personnel, faculty and researchers often lack the knowledge required to identify and respond to emerging cyber threats. This gap can result in unintentional exposure of sensitive data, improper configuration of systems, or delayed reporting of incidents, which are critical under NIS2 requirements (Torgersen *et al.,* 2025).

Additionally, there is a cultural resistance to stringent security policies within academic environments. Universities traditionally promote openness, collaboration, and the free exchange of knowledge, which can conflict with strict access controls, data classification, and compliance procedures (Ulven and Wangen, 2021). Introducing security measures may be perceived as cumbersome or restrictive, leading to inconsistent adoption across departments.

To address these challenges, a gradual and strategic approach is recommended. Universities should prioritize the implementation of Information Security Management Systems (ISMS) and other cybersecurity frameworks in critical areas first, such as research databases, student information systems, and administrative networks. This allows institutions to allocate limited resources effectively while building internal expertise over time.

Investment in continuous training and awareness programs is essential to equip both technical staff and faculty with the knowledge to identify threats, follow best practices, and respond appropriately to incidents. Workshops, online modules, and simulated cyber exercises can help foster a culture of security awareness without compromising the collaborative nature of academic work (Marhad *et al.,* 2024).

Finally, collaboration and knowledge sharing – both internally across departments and externally with other universities or national agencies – can strengthen cybersecurity resilience. By sharing best practices, threat intelligence, and incident experiences, institutions can improve their response capabilities and reduce the learning curve associated with new regulations like NIS2. This cooperative approach ensures that universities not only comply with regulatory requirements but also cultivate a proactive, sustainable cybersecurity posture (ENISA, 2022).

CONCLUSIONS

Higher education institutions are increasingly exposed to complex and evolving cyber threats due to the growing digitalization of academic processes, cloud-based platforms, and the handling of highly sensitive research and personal data. The NIS2 Directive provides a structured legal and regulatory framework, setting clear requirements for risk management, incident reporting, the implementation of security policies, and staff training. Compliance with NIS2 is not only a legal obligation but also a strategic necessity to maintain trust, protect institutional reputation, and ensure uninterrupted academic and research activities (European Commission, 2022).

Implementing internationally recognized cybersecurity management models, such as ISO/IEC 27001, NIST Cybersecurity Framework, COBIT, and maturity models, offers universities practical tools to systematically assess risks, monitor security controls, and continuously improve their cybersecurity posture. These frameworks facilitate alignment with NIS2 requirements, allowing universities to document policies, respond effectively to incidents, and measure progress over time (Calder, 2008).

Moreover, adopting a holistic approach that integrates technical solutions, governance structures, and cultural awareness within the academic community is crucial. This ensures that security measures are not seen merely as regulatory compliance tasks but as essential elements that support innovation, collaboration, and the protection of intellectual and personal assets. By gradually embedding these models into daily operations, universities can overcome challenges related to budget limitations, skill gaps, and cultural resistance, ultimately fostering a resilient cybersecurity environment.

In conclusion, the combination of NIS2 requirements and well-established cybersecurity management models provides higher education institutions with a comprehensive roadmap for strengthening their security capabilities. Beyond compliance, this approach promotes a proactive, adaptive, and sustainable cybersecurity culture, ensuring that universities remain safe, trusted, and capable of fulfilling their academic and research missions in an increasingly interconnected digital landscape.

REFERENCES

Afolalu, O., and Tsoeu, M. S., 2025. Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions. *Future Internet*, 17(12).

Bada, A., Sasse, M. A., and Nurse, J. R. C, 2019. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?., pp. 118-131

Calder, A., 2008. ISO27001 / ISO27002 - A Pocket Guide:IT Governance Publishing.

ENISA, 2022. Cybersecurity Education Initiatives in the EU Member States. Available at: https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states [Accessed 25 04 2026].

European Commission, (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555 [Accessed 20 04 2026].

Ghulam, A., 2025. Cybersecurity Governance and Policy Development in Higher Education Institutions: A Strategic Framework for Resilience and Compliance.

ISACA, 2021. COBIT 2019 Framework: Governance & Management Objectives. Available at: https://www.isaca.org/resources/cobit [Accessed 27 04 2026].

Kitsios, F., Chatzidimitriou, E., and Kamariotou, M, 2023. The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability*, 15(7).

Marhad, S., Goni, S. and Sani, M., 2024. mplementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review. *Environment-Behaviour Proceedings Journal*, (9), pp. 197-203.

Mentzelou, K., Chountalas, P. T., Kitsios, F. C., Magoutas, A. I., and Dasaklis, T. K., 2025. Identifying and Modeling Barriers to Compliance with the NIS2 Directive: A DEMATEL Approach. *Journal of Cybersecurity and Privacy*, 5(4). NIST, 2018. Cybersecurity Framework. Available at: https://www.nist.gov/cyberframework/csf-11-archive [Accessed 02 05 2026].

Papachristofis, K., Vardoulias, G., and Vavousis, K., 2025. Developing cyber-resistivity maturity and scoring framework (CRMSF) for any size of organization. *International Journal of Information Security*, 24.

Riega, J., Riega, Y., Soto, M., and Salas-Riega, J., 2025. Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats. *International Journal of Advanced Computer Science and Applications*, 16(6).

Salam, M., Bakar, K., Ghani, A., and Aman, A., 2026. Cybersecurity in Higher Education Institutions Digitalisation: Addressing Threats and Vulnerabilities. *Sage Open*, 16(1).

Torgersen, L., Noble, E., Ask, T., and Knox, B., 2025. Strengths and Knowledge Gaps Identified From Cybersecurity Education and Training Programs, and the Implications for Operational Technology Personnel in Critical Infrastructures: A Scoping Review. *IEEE Access*.

Ulven, J. B., and Wangen, G., 2021. Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, 13(2).

Zaid, M., 2024. Cybersecurity Education in Higher Institutions: Addressing Challenges and Fostering Awareness