Concept of a Cybersecurity Management Model for Higher Education Institutions

Tatjana Liogienė, Asta Danilevičiūtė, Vaidas Valukonis

Vilniaus kolegija Higher Education Institution, Faculty of Electronics and Informatics

Introduction

International and national requirements governing the activities of higher education institutions (HEIs) drive the digitalization of teaching, research, international cooperation, and data management processes, as well as intensive information exchange.

These **processes** create conditions for the emergence of various cybersecurity (CS) **risk factors**, making it essential to systematically ensure **data** confidentiality, integrity, and availability, as well as regulatory compliance [1].

A literature review revealed a fragmented approach in CS research related to HEIs, with primary attention given to individual technological, organizational, or human aspects. Integrated **organizational-level** CS management models are addressed only to a limited extent, highlighting *the need for a comprehensive model that combines the key CS domains and their interrelationships* [2].

Aim

To develop a conceptual CS management model for HEIs that integrates the institution-specific processes, data, and CS risk factors identified in [1] and addresses the research gap identified in [2] by covering all key CS domains and organizational management levels.

Methods

The proposed conceptual CS management model for HEIs was evaluated and refined using the modified Delphi method. The evaluation involved 10 CS experts from higher education institutions and the public and private sectors, representing scientific, strategic, operational, technological, and regulatory expertise.

Criteria were rated on a 5-point Likert scale (1 = strongly disagree; 5 = strongly agree), and the model was iteratively refined based on expert feedback without sharing aggregated results between evaluation stages. Open-ended expert comments and suggestions for improving the model were also collected.

Results

The proposed model comprises four interrelated *blocks* and nine core *components* derived from HEI-specific processes, data, and CS risk factors, and aligned with the CS management principles established in international standards, legislation, and good practices.

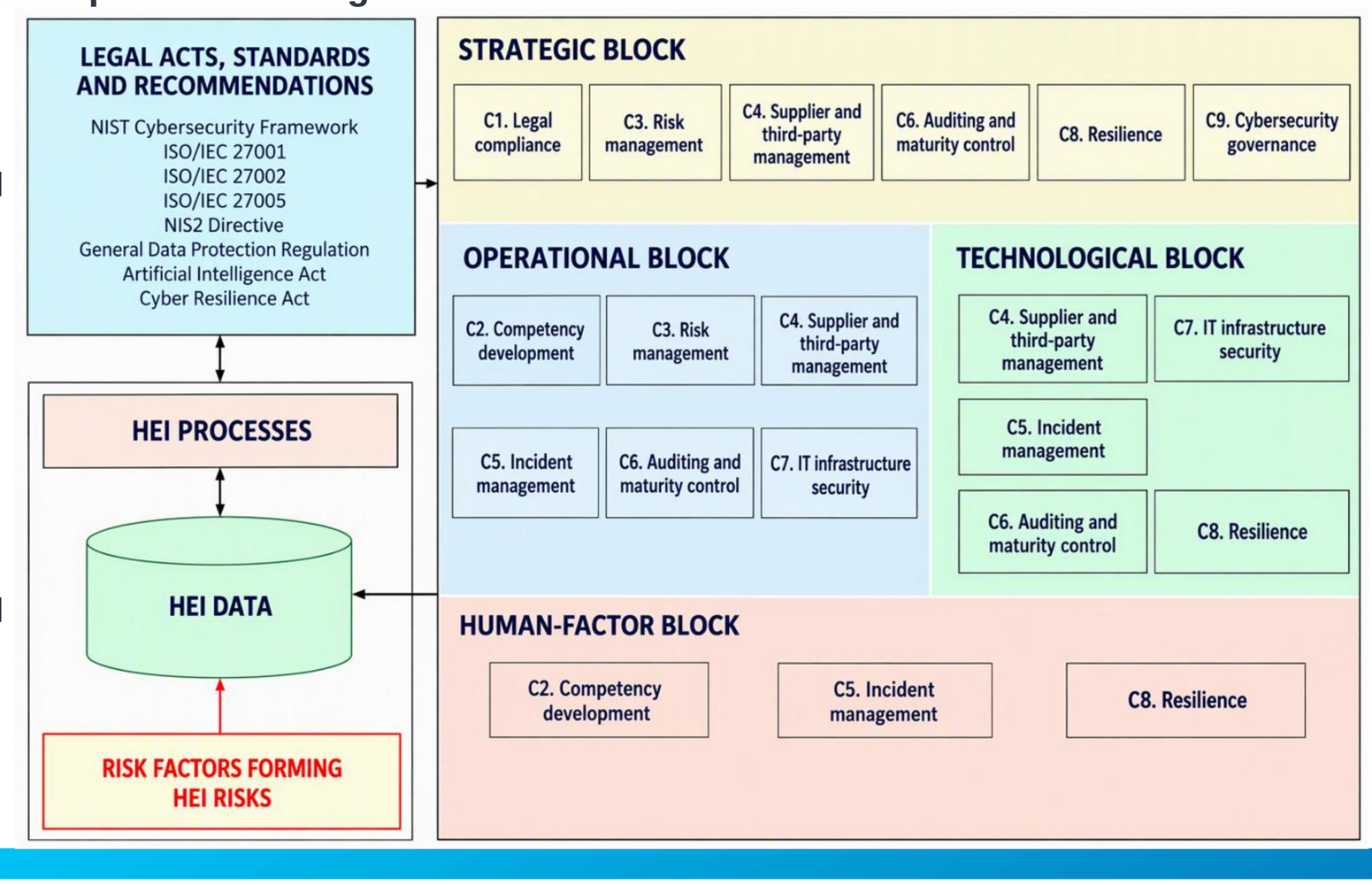
Components are assigned to one or more blocks according to their purpose and level of application, enabling the horizontal and vertical integration of CS management across the institution and reducing the risk of fragmented solutions.

Expert ratings improved following model refinement, and consensus was achieved for all conceptual model evaluation criteria.

Consensus: median ≥ 4, IQR ≤ 1, and ≥ 75% of ratings at 4–5.

The expert evaluation supported the relevance and suitability of the standards, legal acts, and recommendations selected as the basis for the model. It also supported the logical structure of blocks, the adequacy of the identified components, the consistency of their assignment to different blocks, and the model's ability to cover all essential CS domains relevant to HEIs.

Conceptual CS Management Model for HEIs



Conclusions

The proposed conceptual model addresses the fragmented approach identified in previous research by integrating key CS domains and organizational management levels into a unified structure tailored to HEIs.

Expert consensus provides support for the conceptual soundness of the model and its potential to serve as a basis for systematic CS management and enhanced institutional cyber resilience.

Future work will define appropriate controls within each component to address the CS risk factors associated with HEI-specific processes and data.

Comparison of the Results of Stages I and II of the Expert Evaluation

Criterion	Stage I				Stage II			
	Median	IQR	Ratings of 4–5 (%)	Consensus	Median	IQR	Ratings of 4–5 (%)	Consensus
1. The integration of the **standards, legal acts, and recommendations** used in the model is well-founded, relevant, and sufficient for CS management in HEIs.	4	1	80 %	YES	4,5	1	100 %	YES
2. The proposed division into strategic, operational, technological, and human-factor **blocks** is logical and well-founded.	5	1	100 %	YES	5	0	100 %	YES
3. The **components** identified in the model (C1–C9) are sufficient for CS management in HEIs.	4	1	80 %	YES	5	1	90 %	YES
4. The assignment of the **components to individual blocks** is consistent and corresponds to their purpose.	4,5	1	90 %	YES	4,5	1	100 %	YES
5. The model **covers** all essential CS management domains relevant to HEIs.	4	1	80 %	YES	4,5	1	100 %	YES
6. The application of the model can contribute to strengthening the **cyber resilience** of HEIs.	5	1	100 %	YES	**5**	0	100 %	YES

References

[1] Liogienė T., Danilevičiūtė A., Valukonis V. (2026). *Identifying Higher Education Institution-Specific Processes, Data, and Cybersecurity Risk Factors for Strengthening Institutional Cyber Resilience*. In: ICERI2026 Proceedings. IATED.

[2] Liogienė T., Danilevičiūtė A., Valukonis V. (2026). *Cybersecurity Management Research in Higher Education Institutions: A Systematic Literature Review.* In: ICERI2026 Proceedings. IATED.

Acknowledgements

The authors thank the cybersecurity experts who participated in the expert evaluation of the proposed model for their valuable insights and suggestions, which contributed to the improvement of the model.