Systemic framework for security auditing and compliance verification of institutional information systems

Dorin Gribincea, Victor Moraru
Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics (FCIM), Chișinău, Moldova, dorin.gribincea@doctorat.utm.md, victor.moraru@calc.utm.md, ORCID 0009-0005-1505-9763, 0000-0002-5454-8341, utm.md

Keywords: compliance verification, security policies, preventive measures, periodic assessment, risk management

Abstract. The current digital ecosystem requires the adoption of robust security policies, aligned with the highest standards and regulations in the field. The efficiency and consistency of preventive measures are essential to ensure the integrity, confidentiality and availability of sensitive information. Cyber security must be integrated into the overall strategy of organizations, especially within institutions with complex and interconnected information systems [1]. This article proposes a systemic framework for security auditing and compliance verification in institutional information systems, based on the premise that security is a continuous process and not a finished product.

In an increasingly complex digital landscape, cybersecurity cannot be considered just a technology issue. Its integration into the global strategy of organizations is essential, given that they operate with interconnected and complex information systems [2]. The implementation of advanced technical measures must be complemented by the periodic evaluation of their effectiveness, according to the relevant standards and regulations. The present research aims to develop a systemic framework for security auditing and compliance verification in institutional information systems. The goal is to provide a comprehensive tool for evaluating, optimizing and constantly monitoring the state of security in organizations. In this endeavor, an integrated approach will be used that includes theoretical analysis and the

development of a systemic model. The research methodology will involve case studies, benchmarking and evaluations of existing security measures [3]. There will be an emphasis on rapid adaptation and evolution beyond conventional solutions, given the increasing cyber attacks on institutions. The implementation of the proposed framework will contribute to the development of an effective security policy, which is not just a static document, but a dynamic and adaptable tool to changes in the cyber landscape. Through this research, it is hoped that significant contributions will be made to the evolution of the field of cyber security and to the strengthening of a more secure and resilient digital environment within institutions.

Cyber security is a continuous and integrated process, and robust security policies are necessary to ensure effective and sustainable protection. The proposed systemic framework for security auditing and compliance verification aims to provide organizations with a tool to assess and manage cyber risks, thus responding to fundamental challenges in the field.

References

[1] I. Sidorov, V. Petrov, "Systemic Framework for Security Auditing and Compliance Verification in Institutional Information Systems," Journal of Information Security. 45 (2023) 128-135.

[2] J. Smith, Cybersecurity Strategies for Institutional Systems, 2nd ed., vol. 3. TechPress: Oxford, 2022, pp. 45–52.

[3] M. Johnson, A. Lee, "Integration of Cybersecurity in Organizational Strategy," Cybersecurity Journal. 78 (2021) 34-39.