Manufacturing Science and Education 2025

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 68, Issue Special III, August, 2025

FROM REACTION TO PROACTIVITY, A SUSTAINABLE APPROACH OF CYBER RISK ASSESSMENT

Diana HAIMANA, Irina SEVERIN

Abstract: *In an increasingly complex digital environment, organizations face sophisticated cyber threats that challenge traditional risk management models. Although regulatory frameworks such as ISO 27001, NIST, and NIS2 exist, many organizations adopt a compliance-focused approach rather than a proactive one. This study examines the transition from reactive to proactive cyber risk management within a financial organization, highlighting the integration of self-assessment processes and advanced technological solutions. The research identifies key challenges, assesses the impact of implemented measures, and proposes a structured model for enhancing cyber resilience. The findings suggest that aligning IT security with business objectives and leveraging cutting-edge technologies significantly contribute to risk reduction and improved organizational preparedness.*

Keywords: *Cyber risk management, IT security, Artificial Intelligence, Threat detection, Organizational resilience, Risk management, Cyber risk self-assessment.*

1. INTRODUCTION

In an ever-evolving digital landscape, organizations face an exponential increase in cyber threats, which are becoming increasingly sophisticated and challenging to manage. Recent studies highlight that, although numerous regulatory frameworks and international standards exist (ISO 27001, ISO 31000, NIST, DORA, NIS2), they are often compliance-oriented rather than focused on prevention and the strategic integration of cyber risks into business objectives. This limited approach reduces organizations' ability to anticipate and proactively mitigate risks, leading to a reactive management style that responds only after incidents occur.

Another critical issue identified in the specialized literature is the lack of an integrated vision of cyber risks, which are often treated in isolation without being correlated with operational and financial risks. Moreover, traditional risk assessment models struggle to keep pace with technological advancements, particularly in artificial intelligence, machine learning, and advanced data analytics, which could significantly improve threat detection and prevention. Studies also show that decision-makers in organizations tend to underestimate the actual impact of cyberattacks, leading to insufficient resource allocation for protection and recovery

This paper analyzes the current challenges in cyber risk management, highlighting the limitations of existing standards and methodologies. The case study focuses on IT risk assessment within a financial sector company that is part of an international group operating in Europe, America, and Asia. Initially, the organization's approach to cyber risk management was reactive, meaning security measures were implemented post-incident. This strategy led to several challenges, such as the lack of integration of cyber risks into the company’s overall strategy and difficulties in rapidly adapting to new types of attacks.

Starting in 2024, the company adopted a proactive and integrated approach by implementing a structured IT risk self-assessment process. This methodology enables the identification of vulnerabilities before they can be exploited and ensures better alignment of

IT security with business objectives. This paper will explore the impact of the implemented measures and propose alternative solutions, such as integrating self-assessment into risk management and leveraging cutting-edge technological solutions to enhance organizational resilience. The analysis will be based on a literature review and industry examples to outline a more effective cyber risk management model, facilitating the transition from a reactive to a proactive approach.

2. LITERATURE REVIEW

Cyber risk management is an evolving field, particularly due to the rise of sophisticated attacks and increasing regulatory pressures. Recent studies highlight that many organizations remain compliance-focused, neglecting the strategic integration of cyber risks into their business objectives. This literature review provides an overview of existing theories and research, identifying both the limitations of traditional IT risk management models and the benefits of innovative approaches based on self-assessment and artificial intelligence.

According to [1], ISO 27001 and ISO 31000 state that risk management should be a continuous process integrated into organizational strategies. However, many companies adopt a reactive model, where risk analysis is performed occasionally without clear integration into strategic management [2 - 3] recommends a proactive framework for threat detection and prevention, but its application varies significantly depending on organizational maturity.

Studies indicate that traditional approaches present several limitations:

- A compliance-driven orientation, without real anticipation of emerging risks [4].
- Lack of a complete integration between cyber, operational, and financial risks [5].
- Rigidity in assessment processes, preventing rapid adjustments to new attack types [6].
- Underestimation of cyber risks, leading to insufficient resource allocation for protection and recovery [7].

These challenges are confirmed by [8], which suggests that risk assessment must be dynamic and adaptable, rather than merely a formalized audit exercise.

The self-assessment methodology analyzed in Chapter 3 is supported by research demonstrating the benefits of this approach:

- Increased accountability of each department in risk management [9].
- Reduction in security incidents through early vulnerability identification [10].

A critical aspect of this process is the use of performance indicators and global benchmarking, as highlighted in [11]. This enables a better understanding of the maturity level of each local unit compared to group-wide standards.

A current trend in IT risk management is the integration of artificial intelligence (AI) for cyber-attack analysis and prevention. Study [12] shows that AI can improve anomaly detection, compliance management, and threat anticipation.

Summary of Eurostat Report [13] on ICT security incidents and AI adoption in enterprises (2023-2024)

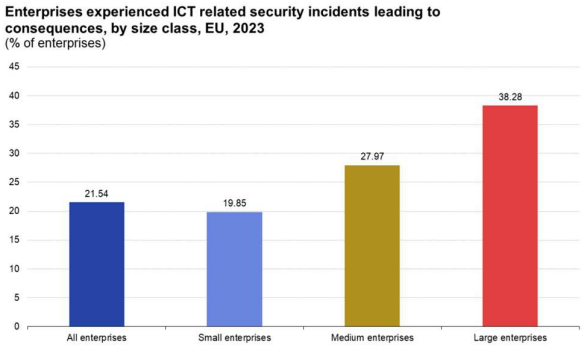

Fig. 1. Enterprises experienced ICT related security incidents leading to consequences, by size class,EU, 2023 (% of enterprises) Source: Eurostat (isoc_cisce_ic)

In 2023, 21.54% of EU enterprises experienced ICT security incidents, leading to issues such as service unavailability, data corruption, or data breaches.

Large enterprises were more affected, with 38.28% reporting incidents, compared to 19.85% of small enterprises.

Security incidents stemmed from both malicious attacks (internal/external) and non-malicious causes (hardware/software failures, employee errors).

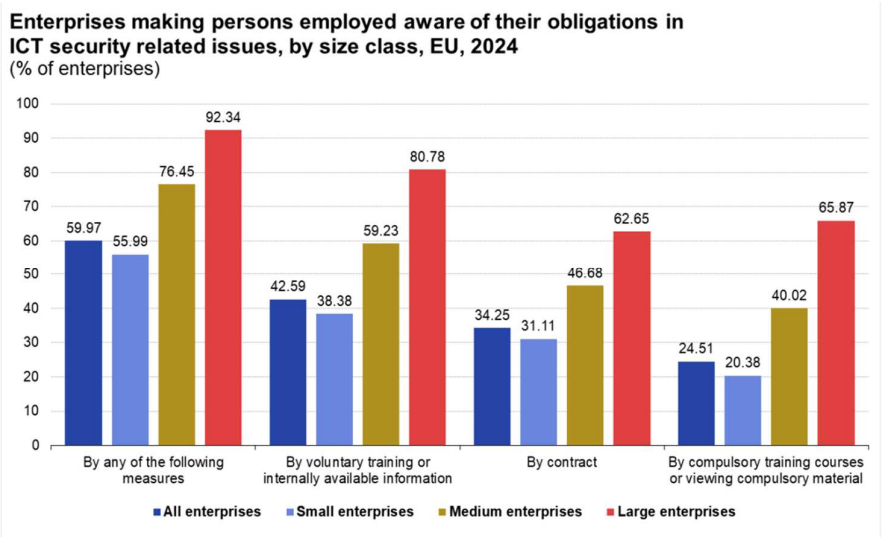

Fig. 2. Enterprises making employed people aware of their obligations in ICT security related issues, by size class, EU, 2024 (% of enterprises) Source: Eurostat (isoc_cisce_ra)

In 2024, 13.48% of EU enterprises (with 10+ employees/self-employed) reported using at least one AI technology.

AI applications included text analysis, machine learning, decision automation, speech recognition, image recognition, natural language generation, and autonomous machine movement.

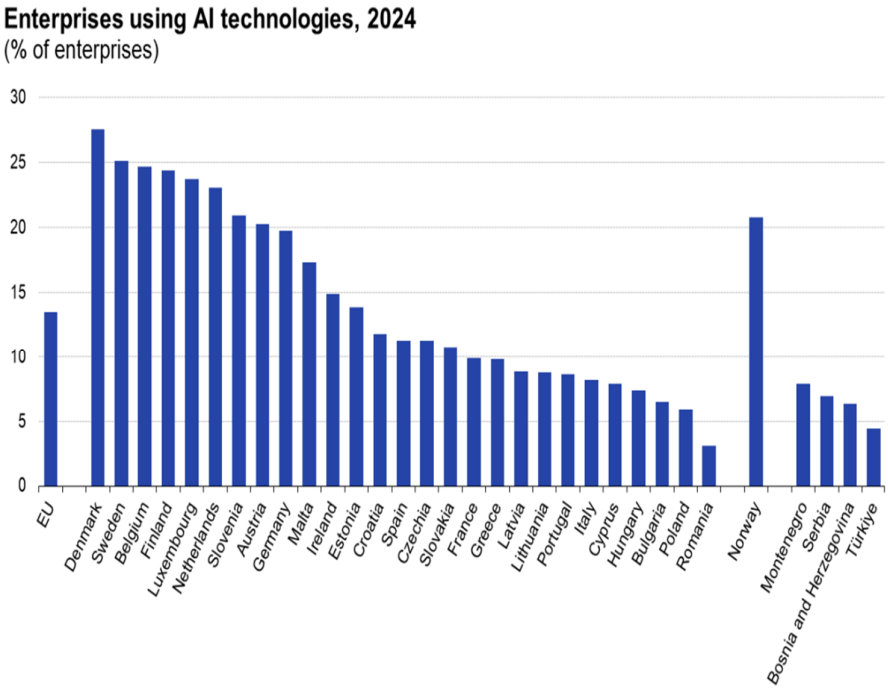

Fig. 3. Enterprises using AI technologies, 2024 (% of enterprises)

41.17% of large enterprises adopted AI, compared to 11.21% of small enterprises, likely due to implementation complexity.

The most commonly used AI technologies were written language analysis (6.88%) and natural language generation (5.41%).

Denmark (27.58%) and Sweden (25.09%) had the highest AI adoption rates, while

Romania (3.07%), Poland (5.90%), and Bulgaria (6.47%) recorded the lowest.

These findings highlight the increasing cybersecurity challenges for enterprises and the growing adoption of AI technologies, particularly among larger businesses.

Chapter 3 of this paper details the methodology implemented for IT risk assessment, based on self-assessment and alignment with business objectives. According to the literature, this method offers significant advantages over traditional models, ensuring faster adaptation to new threats and better integration of risks into organizational strategy.

Chapter 4 analyzes the impact of the implemented measures, and literature confirms the positive outcomes of transitioning from a reactive to a proactive approach. [5] indicates that organizations adopting integrated risk management strategies experience a 30% reduction in the impact of cyber incidents. Additionally, studies on AI in IT security suggest that machine learning-based solutions can improve detection capabilities by up to 40% (Microsoft Digital Defense Report, 2024).

The literature review confirms that traditional IT risk management approaches are insufficient in addressing modern cyber threats. Implementing self-assessment methodologies and integrating AI are essential steps to enhance organizations' ability to anticipate and manage risks effectively.

3. METHODOLOGY – RESEARCH PROCESS FOR IT RISK ASSESSMENT

This research was conducted within a financial sector company that is part of an international group with operations in Europe, America, and Asia. The company operates under a highly regulated environment with strict information security requirements. At the local level, the organization has held ISO 9001 certification since 2018 for quality management and ISO 27001 certification since 2022 for information security.

Until 2024, the company’s approach to cyber risk management was predominantly reactive. Risk analysis was conducted occasionally at a global level, without clear integration into the overall risk management strategy. The risk register was updated primarily post-factum only after security incidents occurred, either locally or within the international group.

This traditional approach generated several significant challenges. Cyber risks were managed primarily to meet regulatory requirements, without a proactive vision for emerging threats, leading to a compliance-driven rather than prevention-oriented approach. The lack of integration of cyber risks into the organizational strategy resulted in IT security being treated as an isolated domain, with no correlation to business objectives. The rigid assessment models used were unable to keep up with new types of cyberattacks and did not allow for rapid adjustments. Moreover, cyber risks were analyzed separately from other operational and financial risks, which could lead to an underestimation of their overall impact on the organization.

Starting in 2024, the company transitioned from a reactive cybersecurity model to a proactive and integrated approach through the implementation of a structured risk self-assessment process. This shift was triggered by the identification of non-compliance findings during internal and external audits, which exposed critical gaps in the previous risk posture. The organization initiated a comprehensive vulnerability identification process, including customized departmental questionnaires, review of internal policies, and analysis of past incidents. This bottom-up process was reinforced by reporting the results to executive leadership, enabling a stronger alignment between cybersecurity and business objectives. As recent literature suggests, a major weakness in cyber risk management is the absence of an integrated vision. [2] emphasize the lack of standardization and coherence across the German cyber insurance market, which reflects broader systemic fragmentation and difficulty in establishing unified risk frameworks across organizations. Additionally, [14] demonstrate that decision-makers often exhibit optimism bias — the cognitive tendency to underestimate the likelihood and impact of cyberattacks — which results in underinvestment in preventive tools such as structured assessments or insurance solutions. One of the key changes was the introduction of

a self-assessment questionnaire distributed across the entire organization, with each department director responsible for completing and validating it in collaboration with process owners.

To ensure comprehensive risk coverage, nine customized questionnaires were developed, each corresponding to a specific business function, with a total of approximately 500 questions. The collected data is analyzed centrally, allowing for an objective assessment of compliance with the organization's policies and standards. A global comparison of the results helps evaluate the maturity level of each local unit in relation to the international group's standards.

Following this process, where deficiencies or low compliance levels were identified, corrective action plans were defined and implemented. This approach enhances adaptability and strengthens the organization's ability to respond quickly to emerging IT security challenges.

4. RESULTS – IMPACT OF THE IMPLEMENTED MEASURES

The transition from a reactive to a proactive approach has generated multiple benefits for the organization. Identifying and managing risks before incidents occur has reduced the likelihood of cyberattacks and improved response times to emerging threats. Another major benefit has been the increased accountability across departments, as their involvement in risk assessment has led to a better understanding of necessary control measures.

The organization’s response capability has significantly improved, with collected data enabling rapid adjustments to IT security strategies based on newly identified risks. Additionally, cyber risks have been integrated into business objectives, enhancing the protection of critical operations.

The new methodology marks a crucial step towards fostering an organizational culture centered on security and prevention, aligning with international best practices in IT risk management.

One of the most significant effects of the new process has been improved accountability within the organization. By distributing self-assessment questionnaires to all business functions and involving department heads in the validation process, a strong IT security culture has been reinforced. This approach has led to a 50% increase in risk awareness among employees, according to internal surveys conducted after implementation.

Mandatory IT security training sessions and courses have been intensified, resulting in a 60% increase in the number of employees trained annually. This initiative has empowered employees to proactively recognize and report potential vulnerabilities, thereby reducing the risk of phishing attacks and data breaches.

Another major benefit of the implemented methodology has been the integration of cyber risks into the company’s overall objectives. By reporting risk assessment results to executive leadership, IT security has been aligned with business strategy, enabling more effective management of technology and security investments. This shift has led to a 25% increase in the budget allocated for IT protection measures, with investments directed toward advanced threat detection solutions, encryption, and continuous monitoring systems.

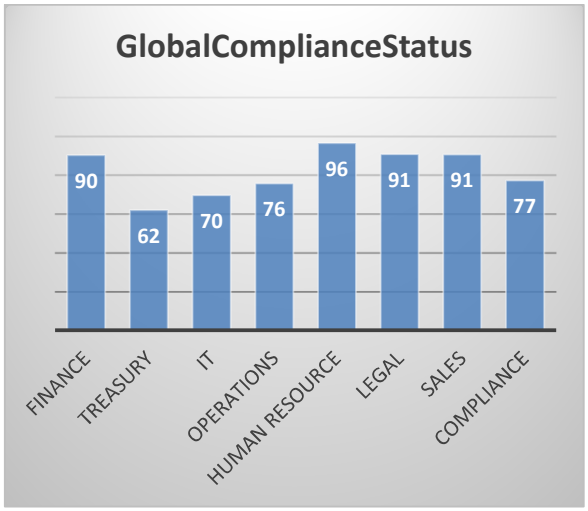

Fig. 4. Global compliance status

The data collected from the self-assessment process confirms that all organizational functions fully completed their SAQ (Self-Assessment Questionnaires), achieving a 100%

completion rate. This demonstrates each department's commitment to adhering to the new process. However, an analysis of compliance scores at the departmental level reveals significant variations.

The Human Resources (96%), Legal (91%), and Sales (91%) functions recorded the highest compliance levels, indicating strong adherence to both security policies and internal regulations. Conversely, the Treasury (62%), IT (70%), and Compliance (77%) departments had the lowest compliance scores, highlighting the need for additional actions to improve processes and align with security standards.

These results emphasize the areas that require increased attention and adjustments in security strategies to ensure a consistent compliance level across all functions within the organization. Action plans for these departments will include:

- Additional security training to reinforce awareness and best practices.
- More frequent security testing to identify and mitigate vulnerabilities.
- Reviewing access and data control policies to enhance security measures.

The analysis of these results, compared to industry benchmarks, confirms the effectiveness of a proactive approach. According to report [5], organizations that integrate IT risk management into their overall strategy experience up to a 30% reduction in the impact of cyber incidents on their operations. Additionally, studies on IT risk management within EU companies [13] indicate that structured self-assessment methodologies contribute to increased risk awareness and the reduction of critical vulnerabilities.

The transition from a reactive to a proactive cybersecurity posture did not occur spontaneously but was triggered by the recognition of non-conformities with existing standards, particularly following internal and external audits. These findings highlighted significant gaps in the organization's ability to anticipate cyber threats and led to an organizational shift in mindset. As a result, the company initiated a structured vulnerability identification process, based on department-level self-assessment, allowing for early detection of security weaknesses and more effective prioritization of risks.

It is important to clarify that the measures proposed in this study have not remained at the planning stage. The self-assessment system has been fully implemented across all departments, with a 100% questionnaire completion rate and validated compliance monitoring. Action plans have been launched in departments with lower security scores, and concrete improvements—such as updated policies, additional training, and stricter access control—have already been initiated. While some actions are ongoing, the operationalization of the proposed methodology has already produced measurable improvements in employee accountability, IT risk visibility, and strategic alignment.

These results offer actionable insights for other organizations aiming to move beyond reactive, compliance-driven models and toward sustainable, preventive cyber risk management.

5. CONCLUSIONS AND FUTURE RESEARCH PERSPECTIVES

This study demonstrates that transitioning from a reactive to a proactive cybersecurity posture, through integrated self-assessment and cross-functional accountability, significantly improves risk identification, mitigation, and overall organizational resilience. While the proposed methodology has been implemented with a 100% completion rate across all departments, the variance in compliance scores indicates that risk maturity levels still differ and require ongoing alignment.

The integration of cyber risks into strategic business planning and the empowerment of department heads have led to a stronger security culture and faster adaptation to emerging threats. Data shows that using a structured self-assessment system has enabled faster identification of vulnerabilities and improved response to digital threats. However, there are still opportunities for improvement to further enhance the efficiency of this process.

Future optimization should focus on leveraging AI and machine learning for predictive risk analytics, aligning cyber risks with financial and operational risk models, and

ensuring continuous employee training. This dynamic, proactive model provides valuable lessons not only for the studied organization but also for other companies aiming to align IT security with strategic objectives in an increasingly complex threat landscape.

To make cyber risk management even more effective, we propose the following actions:

- leveraging Artificial Intelligence (AI) and Machine Learning (ML). These technologies can help automatically detect risks by analyzing large volumes of data and identifying suspicious patterns in real time. This allows the organization to prevent attacks before they become critical issues.
- Integrating cyber risks with operational and financial risks. IT security should be viewed as part of a broader risk management system. By incorporating cyber risks into financial and operational planning, organizations can allocate resources more efficiently and make more informed decisions about protection and mitigation strategies.
- Improving employee training. While progress has been made in increasing risk awareness, continuous training remains essential. Regular security training sessions, phishing simulations, and cyber-attack exercises will help employees recognize and respond to threats more effectively.
- Predictive risk analysis. By using advanced analytics, organizations can anticipate potential threats and implement preventive measures before risks materialize. Additionally, conducting simulated attack scenarios can optimize defensive strategies and improve incident response effectiveness.

To address ongoing cybersecurity challenges, future research should focus on:

- Developing more flexible risk assessment systems that can automatically adapt to organizational changes and emerging threats.
- Exploring how AI can be transparently integrated into IT security, ensuring that automated decisions are understandable and verifiable.
- Creating hybrid risk management strategies that combine traditional security approaches with advanced AI-driven solutions to enhance resilience and adaptability.

By adopting these innovations, organizations can further strengthen their cybersecurity posture and ensure a more dynamic, predictive, and integrated approach to risk management.

6. REFERENCES

[1] *International Organization for Standardization (ISO) ISO 27001: Information Security Management Systems – Requirements*. ISO, ISO 31000: Risk Management – Guidelines. ISO, 2018

[2] Cremer, F., Sheehan, B., Fortmann, M., Mullins, M., Murphy, F., Materne, S., *Bridging the Cyber Protection Gap: An Investigation into the Efficacy of the Cyber Insurance Marke*t, Risk Manage Insurance Review, Wiley, ISSN 15406296, 2024

[3] *Nae of Standards and Technology* (NIST) NIST Cybersecurity Framework (CSF). NIST, U.S. Department of Commerce, 2020 .

[4] *ISACA Risk IT Framework: Balancing Cost, Benefit, and Risk in IT Risk Management*. ISACA, 2020

[5] *Institute of Internal Auditors (IIA) Risk in Focus 2025: Hot Topics for Internal Auditors*. European Confederation of Institutes of Internal Auditing, 2024

[6] Eling, M., Jung, K., *Optimism bias and its impact on cyber risk management decisions*. Risk Sciences, 1 (2024)

[7] Chung, S., *One Size Does Not Fit All: The Value of Information and Coexistence of Rating*, Risk Manage Insurance Review, Wiley, ISSN 15406296, 2024

[8] *Society for Risk Analysis (SRA) SRA Glossary: Terminology and Definitions in Risk Analysis*. Society for Risk Analysis, August 2018

[9] Tolah, A., Malatji, M., *Understanding the Impact of Artificial Intelligence in Shaping Cybersecurity Culture*. Applied Sciences, MDPI, ISSN 2076-3417, 2023

[10] Kim, D., Lee, J., *Development of a Web-Based Tool for Climate Change Risk Assessment in the Business Sector*, Sustainability, MDPI, ISSN 2071-1050, 2016

[11] Björnsdottir, S. H., Jensson, P., Thorsteinsson, S. E., Dokas, I. M., de Boer, R. J., *Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk*, Sustainability, MDPI, ISSN 2071-1050, 2022
[12] Tolah, A., Malatji, M., *Understanding the Impact of Artificial Intelligence in Shaping Cybersecurity Culture*, Applied Sciences, MDPI, ISSN 2076-3417, 2023
[13] *European Commission*, ICT Security in Enterprises, Eurostat, 2024
[14] Meskauskas, Z., Kazanavicius, E., *About the New Methodology and XAI-Based Software Toolkit for Risk Assessment*, Sustainability, MDPI, ISSN 2071-1050, 2022
[15] Eling, M., Jung, K., *Optimism Bias and Its Impact on Cyber Risk Management Decisions,* Risk Sciences, Elsevier, ISSN 2950-6298, 2024
[16] Blokland, P., Reniers, G., *Achieving Organisational Alignment, Safety and Sustainable Performance in Organisations*, Sustainability, MDPI, ISSN 2071-1050, 2021
[17] Poveda-Orjuela, P. P., García-Díaz, J. C., Pulido-Rojano, A., Cañón-Zabala, G., *Parameterization, Analysis, and Risk Management in a Comprehensive Management System with Emphasis on Energy and Performance* (ISO 50001:2018), Energies, MDPI, ISSN 1996-1073, 2020
[18] Selvaseelan, J., *Development and Introduction of the Risk-Sentience Auxiliary Framework (RSAF) as an Enabler to the ISO 31000 and ISO 31010 for High-Risk Environments*, Administrative Sciences, MDPI, ISSN 2076-3387, 2018
[19] ISACA, *Achieving Data Security and Compliance: How to Safeguard Identity, Protect Information, Reduce Risk and Create Value*, ISACA, 2020
[20] Deloitte, 2024 TMT Outlook: *Technology – Preparing for a Return to Growth in the Tech Market*, Deloitte Insights, 2024
[21] Deloitte, 2025 *Technology Industry Outlook*, Deloitte Insights, 2025
[22] Deloitte, *Technology's Impact on Systemic Risk in Financial Services*, World Economic Forum and Deloitte Insights, 2024
[23] Ispas, L., Mironeasa, C., Silvestri, A., *Risk-Based Approach in the Implementation of Integrated Management Systems: A Systematic Literature Review*. Sustainability, 15, 2023
[24] Koen, K., Bouriaud, L., Feindt, P. H., van Wassenaer, L., et al. *Roadmap to Develop a Stress Test for Forest Ecosystem Services Supply*. One Earth, Elsevier, https://doi.org/10.1016/j.oneear.2021.12.009, 2022
[25] European Confederation of Institutes of Internal Auditing (ECIIA) *Risk in Focus* 2025: Hot Topics for Internal Auditors. ECIIA, 2024

De la reactie la proactivitate, optimizarea evaluarii riscurilor cibernetice prin autoevaluare integrate

Intr-un mediu digital tot mai complex, organizatiile se confrunta cu amenintari cibernetice sofisticate, care pun la incercare modelele traditionale de management al riscurilor. Desi exista cadre de reglementare precum ISO 27001, NIST si NIS2, multe organizatii adopta o abordare axata pe conformitate, mai degraba decat una proactiva. Acest studiu analizeaza tranzitia de la un management reactiv al riscurilor cibernetice la unul proactiv, in cadrul unei organizatii financiare, evidentiind integrarea proceselor de autoevaluare si a solutiilor tehnologice avansate. Cercetarea identifica principalele provocari, evalueaza impactul masurilor implementate si propune un model structurat pentru cresterea rezilientei cibernetice. Rezultatele sugereaza ca alinierea securitatii IT cu obiectivele de business si utilizarea tehnologiilor de varf contribuie semnificativ la reducerea riscurilor si cresterea pregatirii organizationale.

Diana HAIMANA, PhD Student, National University of Science and Technology POLITEHNICA Bucharest, Industrial Engineering and robotics, diana.haimana@yahoo.com, 0040729717370
Irina SEVERIN, prof. habil., National University of Science and Technology Politehnica Bucharest, Faculty of Industrial Engineering and Robotics, irina.severin@upb.ro, +40726283850, 313 Splaiul Independenței Street, Sector 6, Bucharest, Romania.