ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-5

THE RELEVANCE OF INFORMATION SECURITY

Shermetov Bunyod Ozodovich[1], Tangriberganova Dildora[2]
[1,2]Technical School No. 4 of Koshkupir Region
Bunyodshermetov917@gmail.com

Abstract. In the era of modern digital transformation, ensuring information security has evolved from a mere technical task into a strategic priority that determines the stability of both nations and the private sector. This article analyzes current challenges in the field of information security, specifically focusing on the vulnerability of digital small and medium-sized enterprises (SMEs) to cyber threats. Beyond traditional technical solutions, the study explores the interplay between information security, the human factor, organizational culture, and governance processes.

By synthesizing international best practices and recent scholarly research from the Scopus database (2012–2024), this study highlights the importance of implementing "maturity models" and "Responsible AI" (RAI) principles to enhance cyber resilience. Furthermore, practical and scientific recommendations are provided for enterprises with limited resources on adopting lightweight security frameworks. The research findings justify the necessity of building an information security system based on a holistic approach, harmonizing people, processes, and technologies.

Keywords: Information security, cybersecurity relevance, digital SMEs, cyber resilience, maturity models, human factor, cyber threats.

Introduction. In the current era of rapid digital transformation and uncertainty, organizations have become constant targets of cyber threats orchestrated by malicious actors. These threats pose significant risks not only to information systems but also to the stability and overall efficiency of business operations. Research indicates that organizations unprepared for crisis situations suffer high levels of financial and operational damage. Consequently, enhancing organizational cyber resilience through Business Continuity Management (BCM) has become more relevant than ever.

Methods. In the modern business landscape, the concept of "Digital SMEs" is gaining particular importance. Digital SMEs refer to enterprises whose core operations rely heavily on cloud platforms, the Internet of Things (IoT), big data analytics, and Artificial Intelligence (AI) tools. Unlike traditional enterprises, digital firms possess a broader "digital footprint," making them more vulnerable to cyber vulnerabilities and risks associated with artificial intelligence. Therefore, information security (InfoSec) is no longer merely a technical issue but a strategic risk that must be managed at the highest level of the business.

The purpose of this study is to analyze the relevance of assessing information and cybersecurity maturity and to explore the possibilities of integrating Responsible Artificial Intelligence (RAI) principles into corporate activities. Throughout the research, the advantages of a holistic approach that considers the information security system in the harmony of people, processes, and technologies will be highlighted. Additionally, practical recommendations for enhancing cyber resilience for Digital SMEs with limited resources will be put forward.

Information security is the practice of protecting information and information systems from unauthorized access, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability (CIA). It involves a holistic approach encompassing three critical components: People, Processes, and Technology.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

VOLUME-6, ISSUE-5

People: Users of information systems are often the first line of defense in maintaining security. This includes employees, management, and third parties who interact with information systems and data.
Processes: Effective processes ensure that security policies are implemented, monitored, and reviewed. These include risk assessment processes, incident response processes, and other similar workflows.
Technology: Technology essentially refers to the tools, systems, and applications used by People to implement or operationalize the Processes for protecting information. Technology is only effective when complemented by robust processes and informed people.

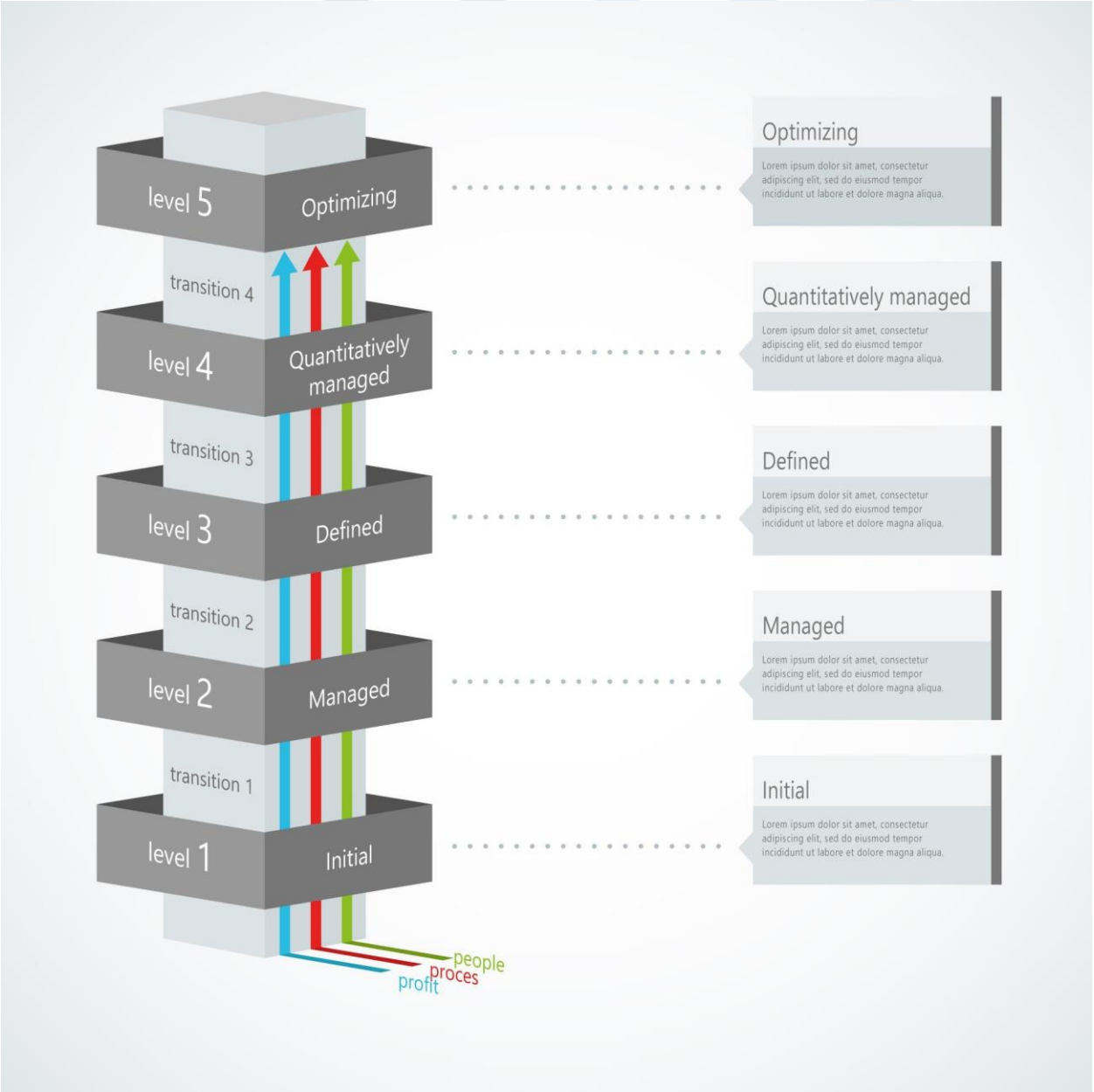

Figure 1. The 5-level development landscape of information security management.

An imbalance among these pillars creates vulnerabilities or loopholes that adversaries may exploit, potentially compromising the Confidentiality, Integrity, and Availability (CIA) of information systems and data.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

VOLUME-6, ISSUE-5

In the current complex and uncertain environment, organizations are increasingly subjected to threats from malicious actors, which can be critical for their business operations and performance. In these settings, organizations are likely to experience a high-cost impact if they are unprepared when a crisis strikes. This is especially true for "Digital SMEs"—enterprises whose core operations rely heavily on digital technologies such as cloud platforms, IoT, big data analytics, and AI tools—for whom information security has become a fundamental necessity. Compared to traditional SMEs, Digital SMEs typically operate with higher levels of technology dependency and broader digital footprints, which broadens their attack surface and increases their exposure to inherent vulnerabilities in the digital tools used. Therefore, information security is no longer merely an information technology (IT) problem; it has become a strategic business risk that must be handled with due care at the highest level of the organization.

Information Security (InfoSec) requires a holistic approach to ensure the CIA triad of information and relies on three critical pillars: people, processes, and technology. While people are often considered the first line of defense, non-technical barriers—specifically the "human factor" such as employee awareness and organizational culture—are frequently overlooked in existing studies. An imbalance among these pillars creates vulnerabilities that adversaries can exploit. Consequently, organizations should utilize the concept of maturity assessment to gain a comprehensive understanding of their security capabilities and drive continuous enhancement of their security posture. Maturity models provide a structured framework to evaluate current capabilities and identify a logical path for improvement, moving from an "Initial" state to an "Optimizing" level of efficiency.

The integration of InfoSec in Responsible AI (RAI) implementations serves to increase competitiveness and ensure resource efficiency. Adopting lightweight maturity models allows small and medium-sized enterprises to build sustainable, secure, and ethical digital practices tailored to their unique needs. This approach assists enterprises in identifying vulnerabilities and developing a risk-based strategic defense against evolving cyber threats. Ultimately, the synthesis of InfoSec and RAI becomes a pivotal factor in ensuring an enterprise's long-term stability and innovative development within the digital economy.

To achieve the research objectives, a Systematic Literature Review (SLR) approach was utilized. This approach provides a systematic, explicit, and reproducible method for identifying, selecting, evaluating, and critically appraising the existing body of completed and recorded research.

Drawing on guidelines for creating a comprehensive SLR and the experiences of other authors, a specific SLR process was defined for this study. As suggested by previous research, the SLR was conducted in accordance with PRISMA guidelines to ensure scientific rigor and minimize bias in the findings. To facilitate the identification, screening, visualization, and bibliographic analysis of the study, Mendeley Reference Management Software and Microsoft Excel were utilized.

As illustrated in Figure 2, this process consists of three main steps: planning the review, conducting the review, and reporting the review.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-5

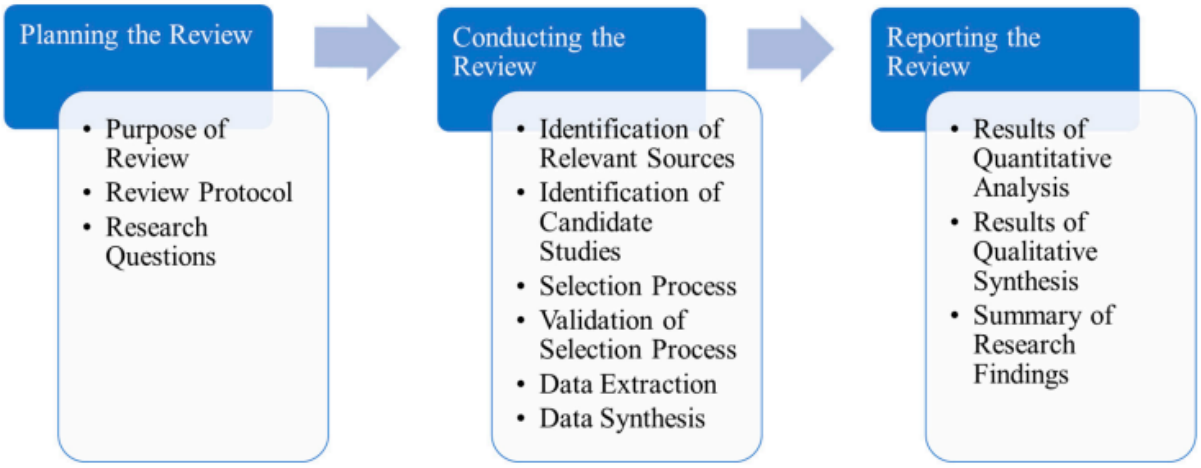

Figure 2. Systematic literature review process used in the study

The main tasks related to planning the review are determining the purpose of the review and the scope of the study, developing a review protocol, and defining the research questions. The tasks associated with conducting the review are the identification of relevant sources, the identification of eligible studies (i.e., candidate studies), the selection process (i.e., the application of inclusion and exclusion criteria to determine the final collection of relevant studies), the validation of the selection process by independent reviewers, data extraction, and data synthesis.

Review reporting is the final step in the creation of a Systematic Literature Review (SLR) and involves the systematic and smooth reporting and writing up of the results, so that the entire process is scientifically reproducible. The results of the review can be presented in the form of a quantitative analysis and qualitative synthesis of SLR findings.

This study demonstrates that within the context of the modern digital economy, the role of information security has evolved from mere technical protection measures into a strategic business necessity. For Digital SMEs that rely on cloud technologies, the Internet of Things (IoT), and Artificial Intelligence (AI) during the process of digital transformation, ensuring cyber resilience is the most pressing issue related to the enterprise's survival. The conducted analyses prove that relying solely on technological tools to ensure information security is insufficient; the effectiveness of the system is directly dependent on a holistic approach based on the balance between people, processes, and technology.

The research findings confirm that cybersecurity maturity assessment models serve as a logical and systematic roadmap for enterprises to incrementally enhance their defensive capabilities. In particular, the integration of Responsible Artificial Intelligence (RAI) principles into the information security system guarantees not only technical security but also compliance with ethical and legal standards in data management. Implementing lightweight maturity models for small and medium-sized enterprises with limited resources allows for the construction of effective and sustainable security strategies tailored to their unique needs.

In conclusion, accepting information security as a continuously evolving process and placing the human factor at its center is the primary factor for Digital SMEs to remain competitive in the global market and increase their resilience against cyber threats. Future research should be directed toward more deeply adapting these maturity models according to the specific characteristics of various economic sectors.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

VOLUME-6, ISSUE-5

References

[1] J. De Matteis, G. Elia, and P. Del Vecchio, "Business Continuity Management and Organizational Resilience: A Small and Medium Enterprises (SMEs) Perspective," *J. Conting. Crisis Manag.*, vol. 31, pp. 670–682, 2023.

[2] R. Bhamra, S. Dani, and K. Burnard, "Resilience: The Concept, a Literature Review and Future Directions," *Int. J. Prod. Res.*, vol. 49, pp. 5375–5393, 2011.

[3] J. Groenendaal and I. Helsloot, "Cyber Resilience during the COVID-19 Pandemic Crisis: A Case Study," *J. Conting. Crisis Manag.*, vol. 29, pp. 439–444, 2021.

[4] M. A. Sánchez and M. De Batista, "Business Continuity for Times of Vulnerability: Empirical Evidence," *J. Conting. Crisis Manag.*, vol. 31, pp. 431–440, 2023.

[5] M. N. Y. Marican, S. A. Razak, A. Selamat, and S. H. Othman, "Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review," *IEEE Access*, vol. 11, pp. 5442–5452, 2023.

[6] C. Schmitz, M. Schmid, D. Harborth, and S. Pape, "Maturity Level Assessments of Information Security Controls: An Empirical Analysis of Practitioners Assessment Capabilities," *Comput. Secur.*, vol. 108, p. 102306, 2021.

[7] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement," *Int. J. Surg.*, vol. 8, pp. 336–341, 2010.

[8] M. J. Page *et al.*, "The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews," *BMJ*, vol. 372, p. n71, 2021.

[9] T. Mettler, "Maturity Assessment Models: A Design Science Research Approach," *Int. J. Soc. Syst. Sci.*, vol. 3, pp. 81–98, 2011.

[10] T. Mettler, P. Rohner, and R. Winter, "Towards a Classification of Maturity Models in Information Systems," in *Management of the Interconnected World*, A. D'Atri, M. De Marco, A. M. Braccini, and F. Cabiddu, Eds. Heidelberg, Germany: Physica-Verlag HD, 2010, pp. 333–340.

[11] P. Virkkala, M. Saarela, K. Hänninen, J. Kujala, and A.-M. Simunaniemi, "Business Maturity Models for Small and Medium-Sized Enterprises: A Systematic Literature Review," *Management*, vol. 15, pp. 137–155, 2020.

[12] J. Becker, R. Knackstedt, and J. Pöppelbuß, "Developing Maturity Models for IT Management," *Bus. Inf. Syst. Eng.*, vol. 1, pp. 213–222, 2009.