Practical toolkit for self-diagnosed information security based on a risk-oriented approach*

Svitlana Shevchenko[1,*,†], Yuliia Zhdanova[1,†], Olena Nehodenko[1,†], and Oleksii Kiia[1,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine*

Abstract

Modern network infrastructure is characterized by high heterogeneity, scalability, and complexity, which complicate ensuring stable operation in the face of dynamic threats. In particular, unauthorized influences pose a special danger – hidden or undeclared actions that traditional signature analysis methods cannot detect. This article proposes a method for detecting unauthorized influences in network interactions based on intelligent traffic analysis. The problem lies in the insufficient effectiveness of traditional methods in detecting new or hidden attacks. The study aims to develop a hybrid approach that combines traffic clustering, analytical indices, and eXplainable Artificial Intelligence (XAI). Self-Organizing Maps (SOMs) are used for traffic cluster analysis, and a criticality index and derivative are used to assess the impact of features. SHAP and LIME methods are used to interpret the results. Experiments are conducted on real-world network datasets. Improvements in accuracy metrics (F1, TPR, MCC) are obtained compared to baseline models. The scientific novelty lies in the combination of SOM clustering with index-based impact assessment and explainable traffic analysis. The method is suitable for implementation in intrusion detection systems and for improving the resilience of corporate networks to atypical threats.

Keywords

explainable artificial intelligence, XAI, self-organizing map. SOM, anomaly detection, cyber influence modeling, intelligent intrusion detection, critical feature analysis, cyber threats, unsupervised learning

1. Introduction

The development of machine learning and artificial intelligence methods has made it possible to optimize routine actions in the field of information and cyber security [1]. At the same time, using information technologies, cybercriminals are improving their methods and criminal activities by scaling cyberattacks, increasing their speed and efficiency, which contributes to expanding the range of threats that organizations face. Small and medium-sized organizations (SMOs) remain the most vulnerable segment [2, 3]. Analysis of analytical reports [4] revealed a rapid increase in the number of attacks related to impersonation, session hijacking, token theft and exploitation of vulnerabilities in cloud supply chains. Attackers are increasingly using the "Living off the Land" (LOTL) tactic, using legitimate software. British statistics for 2025 [5] confirm this trend: attacks were recorded in 41% of microbusinesses and one in two small enterprises. The consequences of such incidents are often fatal: 60% of small sector companies are forced to cease operations within six months of a serious attack [6].

According to the International Digital Trust 2025 Analytical Study [5], cybersecurity is a priority for businesses, but only 2% of organizations have implemented measures to ensure cyber resilience at all levels. There are problems with the quantitative assessment of cyber risks: 47% of respondents are concerned about the reliability and validity of the results of such an assessment, and 39% are concerned about the uncertainty of the assessment. The dynamism and multi-vector nature of malware has prompted researchers and practitioners to develop a wide range of conceptual approaches to ensuring data integrity, availability, and confidentiality, ranging from

* *CSDP'2026: Cyber Security and Data Protection, May 7, 2026, Lviv, Ukraine*

* Corresponding author.

† These authors contributed equally.

s.shevchenko@kubg.edu.ua (S. Shevchenko); y.zhdanova@kubg.edu.ua (Y. Zhdanova); o.nehodenko@kubg.edu.ua (O. Nehodenko); oskiia.fitm24m@kubg.edu.ua (O. Kiia)

0000-0002-9736-8623 (S. Shevchenko); 0000-0002-9277-4972 (Y. Zhdanova); 0000-0001-6645-1566 (O. Nehodenko); 0009-0003-4105-8081 (O. Kiia)

deterministic protection models to probabilistic ones using risk-based technology. However, the complexity of most risk-based security systems makes their application possible only for large businesses with significant resources and a large staff of qualified information security specialists. Therefore, MSOs need solutions that are cost-effective, easy to manage, and consistent with their limited financial and human resources [7, 8].

2. Literature overview

Small and medium-sized businesses are the foundation of the global economy, generating more than half of the world's gross domestic product and providing employment for the majority of the population. Given such a large-scale impact, the implementation of a risk-based approach to information and cyber security in SMEs has become critical. This has led to the emergence of numerous scientific and practical developments aimed at improving the system of protecting this sector from cyber threats and making effective decisions, building the cyber resilience of the organization.

Cyber resilience is commonly defined as the organizational, technological, and human capacity to anticipate, detect, withstand, recover from, and adapt following cyber incidents [2]. Consequently, risk management in information systems must evolve from a narrow focus on cybersecurity toward a broader paradigm of cyber resilience [9].

Maturity models are frequently employed to assess the current state of an organization's resilience [2]. For example, [10] introduced a spirally structured maturity model that enables rapid, low-cost assessment of organizational resilience. Unlike conventional models with five or six levels, this approach incorporates only three security levels, each certified independently. The model unfolds across three phases: (1) assessment of current and projected maturity levels, (2) risk analysis, and (3) ISMS Generation, which provides solutions derived from a structured library (including 4 technical instructions, 25 regulations, 65 patterns, 50 procedures, and 35 registers). Practical validation of this tool, as reported in [11], demonstrated high levels of satisfaction among SMO managers.

A complementary approach was proposed in [12–14], which integrates qualitative and quantitative methods for risk assessment. The algorithm begins with threat identification through SWOT analysis, followed by a flexible choice of tools—statistical methods when sufficient data are available, or expert evaluation otherwise. Scenario modeling and probability estimation are supported by Monte Carlo simulations.

Simplification remains a recurring theme in SMO-focused research. The authors of [15] emphasized that risk management systems must be streamlined, offering a theoretical justification for 14 variables within the conceptual SMERMF framework. Similarly, [16] advanced a four-stage cyber resilience methodology, implemented as the CR-SAT web application. One limitation noted was the necessity of supplementary services and guides to support SMOs in applying the methodology effectively.

Applied digital tools have also been explored. For instance, [17] described the use of a URL classifier to counter phishing and assess risks based on threat intelligence and LCCI. This solution, however, was limited to three primary threats—malware, web attacks, and phishing—and relied on NIST CSF and ISO 27001/2 frameworks. In [18], the authors introduced a web service that replaces subjective managerial judgments with objective threat analysis. By responding to structured questions, users receive automatically generated, personalized action plans, thereby mitigating the problem of organizational "self-deception" and enhancing audit reliability.

Further contributions include the GestionAVR application [8], designed to integrate structured risk management processes for SMOs. Testing in the engineering sector revealed positive outcomes, such as reduced planning time and improved vulnerability detection. Nonetheless, the tool lacked synchronization with international standards and automated reporting features.

Human factors remain a critical dimension of resilience modeling. The study in [19] proposed two complementary methodologies: customer journey modeling (CJML diagrams) and secure

systems modeling. A key advantage of these approaches lies in their ability to facilitate communication between cybersecurity experts and non-technical personnel.

At the policy level, the European Union Agency for Cybersecurity (ENISA) introduced in 2024 a practical tool for assessing SMO cybersecurity maturity. Based on structured questionnaires, the tool enables self-diagnosis and generates tailored recommendations aligned with best practices [7].

A large number of studies confirm the relevance and importance of this topic. However, the theoretical nature of many scientific methods complicates their practical application, requiring complex adaptation to the context of the organization. As practice shows, there is no universal solution for building cyber resilience of organizations, because it is they who determine and implement those technologies that satisfy their resource constraints and strategic priorities.

3. Research method

The development of a practical toolkit for self-diagnostics of information security of an organization based on a risk-based approach is based on regulatory support in the IS system, namely, NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, CIS Controls v8 [20–23]. The structured survey was carried out using the NIST CSF 2.0 framework as a basic measuring tool, COBIT 2019 was used as a mechanism for determining the target state through prioritization of business processes, ISO/IEC 27001:2022 as a reference for documented controls, CIS Controls v8 as additional practical detailing for small and medium-sized organizations (SMEs).

The process of organizing the work of the expert group was developed using SWOT analysis, which allowed converting the qualitative characteristics of the functioning of the SMEs into a structured list of critical influence factors. This provides a solid foundation for further quantitative analysis and strategic planning of the organization's cyber resilience.

The architecture and processes of this toolkit are presented using a use case diagram that shows the role of information system experts and the main functions of this system, and an activity diagram that describes the four-phase process of assessing the organization’s cyber maturity.

Given the limited resources of small and medium-sized businesses, it is recommended to use Microsoft Excel as a basic tool for internal security audits.

4. Main material

The theoretical basis of the practical toolkit for self-diagnosis of an organization's information security based on a risk-based approach is the integration of four IS frameworks: NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, CIS Controls v8, a comparative analysis of which is presented in Table 1. Despite the obvious advantages of recognized standards, their high abstraction and vagueness of formulations complicate practical application for small and medium-sized businesses [9, 24]. Also a problem is the large number of related issues in each document. Therefore, first an analysis of the official mappings (Crosswalks) of the relevant frameworks was conducted:

1. Official mapping of CIS Controls v8.1 (153 Safeguards) to NIST CSF 2.0 (106 categories) [25]—45 Safeguards are explicitly mapped (29.4% of the total) and 108 Safeguards are partially mapped (70.6%). The largest gaps are observed in the Protection and Detection functions—precisely those areas where technical CIS controls are most detailed and practically valuable for organizations.

2. Official mapping of NIST CSF to ISO/IEC 27001:2022 [26]—ISO Annex A coverage: 68 out of 93 controls (73%); mandatory section coverage: 21 out of 33 controls (64%). The biggest gap is that 25 Annex A controls remain without a direct mapping in the NIST CSF.

3. Official mapping of NIST CSF 1.1 to COBIT 2019 [27]—since the official mapping was for NIST 1.1, a transition mapping was performed to NIST 2.0. The biggest problem was that NIST CSF 2.0 has 106 subcategories compared to 98 in version 1.1—new elements (especially the Governance function) do not have direct equivalents in the COBIT mapping.

Table 1
Comparative analysis of leading cybersecurity frameworks

Criterion	NIST CSF 2.0	ISO/IEC 27001:2022	COBIT 2019	CIS Controls v8
Version	2.0	27001:2022	2019	v8.1 (2024)
Release Year	February 2024	October 2022	April 2019	June 2024
Primary Focus	Risk-oriented cyber risk management	Information Security Management System	IT governance and business–IT alignment	Practical actions for protection against cyber threats
Structure	6 functions → 23 categories → 106 subcategories	Clauses 4–10 + Annex A (93 controls)	5 domains → 40 governance objectives	18 controls → 153 safeguards → 3 implementation groups
Number of Elements	106 subcategories	93 controls in Annex A	40 governance and management objectives	153 safeguards
Flexibility	High (adaptive framework)	Medium (requires strict structure)	High (11 design factors)	High (3 implementation tiers)
Certification	No (voluntary framework)	Yes (international certification)	No (reference standard)	No (set of best practices)
Target Audience	Any organizations (government, business, SMEs)	Organizations requiring certification	IT departments, CIOs	SMEs with limited resources
Approach	Strategic, outcome-oriented	Process-based, requirement-oriented	Governance-focused, management-oriented	Practical, action-oriented
Key Advantages	Flexibility, universality, broad recognition	International recognition, certification	Business–IT alignment, metrics	Ease of implementation, SME orientation
Key Limitations	Lack of certification, requires adaptation	Certification cost, rigid structure	Implementation complexity, requires maturity	Less detail for complex environments

A comparison of typical gaps between CIS Controls and ISO 27001 is presented in Table 2.

Table 2
Statistics of typical gaps

Type of Gap	ISO 27001 (of controls, %)	CIS Controls (of safeguards, %)
Different levels of abstraction	12	36
New elements in frameworks	10	8
Industry-specific aspects	5	27
Total requiring refinement	29	71

The formation of a holistic matrix of interrelationships required the elimination of the identified discrepancies through systematic expert verification and refinement based on semantic analysis, the use of the Security Function as a navigational reference point, and expert validation. Each established connection was checked by a group of three experts with experience in implementing all four frameworks. A connection was considered valid if at least two of the three experts confirmed it. The results of the refinement are presented in Table 3.

Thus, the overall correspondence matrix is an Excel file “NIST 2.0 Master Mapping” with 106 rows (NIST subcategories) and 7 columns:

1. NIST 2.0 Function.
2. NIST 2.0 Category.
3. NIST 2.0 Subcategory.

4. NIST CSF 1.1 (for backward compatibility).
5. COBIT 2019 (31 relevant objectives).
6. ISO 27001:2022 (126 controls).
7. CIS Controls v8.1 (153 Safeguards).

Table 3
Statistics and examples of mapping refinement

Framework	Official Coverage	Refined/ Extended	Example of Refinement
ISO 27001:2022	66/103 (64%)	+37	• NIST PR.AA-04 *"Identity and credential lifecycle is managed,"* direct control of access lifecycle. • NIST PR.AA-01 *"Identities and credentials for authorized users are managed,"* broader requirement, ISO specifies the termination scenario.
COBIT 2019	40/40 (of which 31 relevant)	Selection and adaptation	From 40 objectives, 31 were selected: • Nine objectives purely related to IT operational management were excluded (e.g., BAI07 *"Manage change acceptance and transitioning"* – focused on software change management rather than security); • Focus placed on EDM, APO (risk management), BAI (secure development), DSS (incident management).
CIS Controls v8.1	45/153 (29.4%)	+108	For CIS 17.1 (*Designate Incident Response Roles*), official mapping links only to the NIST CSF 2.0 "Respond" function, without specifying a subcategory. Refinement process: 1. Analysis of description: "roles and responsibilities," "response coordination". 2. Search within the Respond function (13 subcategories): • RS.MA-01 *"Incident response activities are coordinated,"* management of the response process. • RS.AN-01 *"Incident data and metadata are collected."* – Narrower part of the response process. 3. Two links established: CIS 17.1 ↔ RS.MA-01, RS.AN-01.

Each cell contains a list of corresponding controls from other frameworks separated by ";". For example, for NIST PR.AA-01, the CIS column might contain "4.3; 4.7; 5.2; 5.3; 6.6" indicating all relevant Safeguards.

In this model, the central measurement instrument is NIST CSF 2.0.

The mechanism for assessing cyber maturity consists of four phases, whose sequential implementation enables the determination of the current state of organizational cyber maturity and the development of a roadmap for improvement.

Phase 1. Formation of the expert group and organizational context. The expert group includes specialists in IT, cybersecurity, risk management, law, and management of key business areas. Through structured discussion supported by SWOT analysis [28], the group conducts a comprehensive examination of the organization's strategic objectives, critical processes, and

regulatory environment. The outcome of this stage is the formalization of the Organizational Context—a foundational document that defines the parameters for subsequent evaluation.

Phase 2. Assessment of the current state (As-Is) using NIST CSF 2.0. The evaluation process is based on a structured questionnaire covering all 106 subcategories of the NIST CSF framework. The organization responds to 92 questions distributed across 18 business-oriented information security processes. Based on these responses, the system automatically calculates the score for each process as the average of all answers within that process on a 0–4 scale. These values are then used by the algorithm to compute the overall maturity level on a 0–5 scale. To ensure data reliability, an expert verification stage is included: the group of specialists compares automated indicators with the actual state of security and adjusts them according to the specifics of the organizational environment.

Phase 3. Determination of the target state (To-Be) through COBIT 2019. Using the COBIT methodology, the expert group identifies priority governance objectives within five key domains. Through a developed correspondence matrix, these objectives are automatically converted into target maturity indicators for the relevant NIST CSF subcategories, thereby enabling the formation of a substantiated target cybersecurity profile for the organization.

Phase 4. Gap analysis and development of the improvement roadmap. The system performs an automated comparison of the current and desired security states, generating a detailed list of discrepancies. On this basis, a multi-standard improvement strategy is constructed, incorporating cross-framework guidance: enhancing maturity according to NIST, optimizing management controls under ISO 27001, and implementing practical safeguards from CIS Controls. To ensure the feasibility of the proposed measures, experts adapt the roadmap by considering the available budget, human resources, and the strategic importance of organizational units.

To illustrate the main stages of the cyber maturity assessment process, as well as the decision-making logic in the control phases, Figure 1 presents a structural-logical model based on the integration of NIST CSF 2.0, COBIT 2019, ISO/IEC 27001, and CIS Controls.

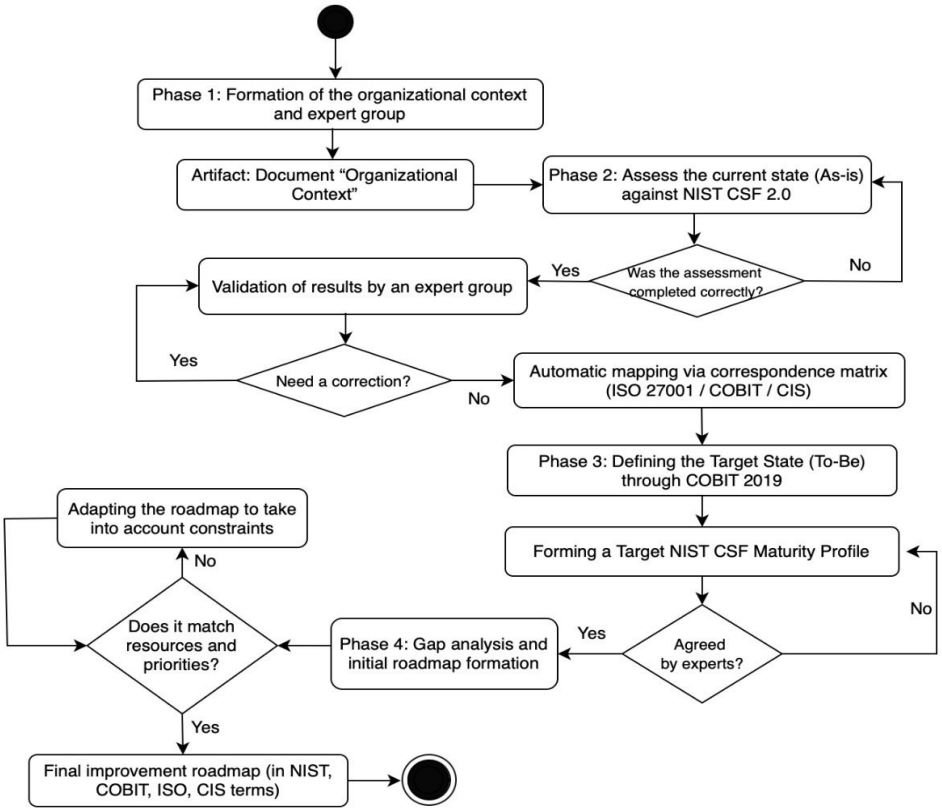

Figure 1: UML activity diagram of the four-phase cyber maturity assessment process

The main scenarios of user interaction with the cyber maturity assessment system are presented in Figure 2 using a use case diagram, which shows the role of experts with the information system, as well as the main functions of this system.

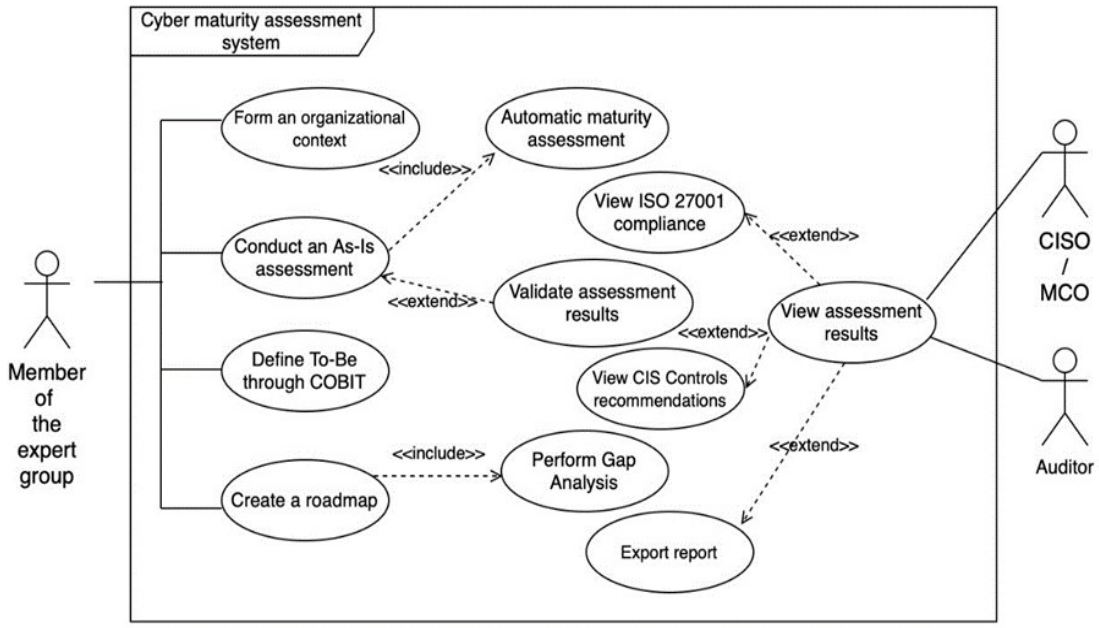

Figure 2: Cyber maturity assessment system use case diagram

The developed toolkit offers a systematic approach to cyber maturity assessment, the key advantage of which is the creation of a "single window" for simultaneous auditing according to several international standards [29, 30]. Thanks to the use of a correspondence matrix, it is possible to achieve significant resource optimization: the assessment results are automatically translated between different frameworks, which eliminates the need to duplicate efforts when checking identical requirements within NIST, ISO, COBIT and CIS. The high scalability of the solution deserves special attention: the tool is equally effective for both small and medium-sized businesses (in particular, due to the focus on CIS IG1) and large corporations that require comprehensive management according to COBIT principles. Along with the above advantages, the use of the tool has certain specific aspects that should be taken into account. In particular, to achieve the integrity of coverage, the authors carried out a deep methodological adaptation of official mappings, which makes the tool unique, but requires an understanding of its internal logic. It is also important to note that the formed roadmap is a basis for improvement, but it does not replace a full-fledged certification audit (for example, for the ISO 27001 standard), which requires a separate detailed study of the documentary base. Finally, despite the high level of automation, the application of the "Human-in-the-Loop" principle remains critically important: expert validation is a prerequisite for the correct interpretation of results in a specific organizational context, where algorithmic assessment may not take into account atypical business risks [31–33]. Similar AI-oriented approaches are also relevant for web application security, where intelligent models support vulnerability analysis, attack detection, and explainable risk-oriented decision-making [34].

5. Conclusions

Modern requirements for information and cybersecurity oblige organizations to maintain simultaneous compliance with a number of leading information security frameworks. However, the practice of conducting isolated audits for each standard creates the problem of duplication of functions and excessive resource burden, which is a significant barrier to IS self-assessment for small and medium-sized businesses. In response to these challenges, a practical toolkit for self-diagnosis of an organization's information security was developed based on a risk-based approach, which integrates the following solutions:

- Convergence of frameworks (NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, CIS Controls v8) to develop a cross-standard matrix that provides a single assessment cycle and eliminates redundancy of procedures.
- Automation of structured questionnaires, which minimizes the subjective factor and increases the reliability of the obtained cyber maturity indicators.
- Hybrid validation of results using the "Human-in-the-Loop" principle to adapt the assessment to the unique business needs of the organization.
- Risk analysis by experts based on SWOT analysis to identify internal strengths and external challenges obtained during an automated survey.

The results of this study have practical value for enterprises that seek to simplify information and cyber security risk management through a unified assessment. A self-diagnostic tool for determining the level of cyber maturity through a multi-standard assessment using several frameworks simultaneously without duplication is a proactive support for SMOs that have limited material, technical and human resources. The proposed approach also allows cybersecurity specialists to minimize time spent during comprehensive IS audits.

The introduction of research materials into the educational process of Borys Grinchenko Kyiv Metropolitan University for students of the F5 specialty Cybersecurity and Information Protection contributed to a deeper assimilation of theoretical material and the formation of sustainable practical skills in implementing a risk-oriented approach in security systems.

It is planned to develop a web application as an alternative tool that will provide variability between web solutions and Excel tables.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] Y. Kostiuk, et al., Models and Technologies of Cognitive Agents for Decision-Making with Integration of Artificial Intelligence, in: Modern Data Science Technologies Doctoral Consortium (MoDaST), vol. 4005 (2025) 82–96.

[2] J. F. Carías, et al. Systematic Approach to Cyber Resilience Operationalization in SMEs, IEEE Access 8 (2020) 174200–174221. doi:10.1109/ACCESS.2020.3026063

[3] A. Chidukwani, S. Zander, P. Koutsakis, A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations, IEEE Access 10 (2022) 85701–85719. doi:10.1109/ACCESS.2022.3197899

[4] Guardz, Small Business Cyberattack Surge: Attacks Nearly Double in 2025. PR Newswire (2025). https://www.prnewswire.com/news-releases/small-business-cyberattack-surge-attacks-nearly-double-in-2025-guardz-reports-302560327.html

[5] UK Government, Cyber Security Breaches Survey 2025 (2025). https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025

[6] BD Emerson, Must-Know Small Business Cybersecurity Statistics for 2025 (2024). https://www.bdemerson.com/article/small-business-cybersecurity-statistics
[7] ENISA, Cybersecurity Maturity Assessment for Small and Medium Enterprises (2024). https://www.enisa.europa.eu/tools/cybersecurity-maturity-assessment-for-small-and-medium-enterprises
[8] D. Rusu, M. Mantulescu, Development of an Application-based Framework for Information Security Management in SMEs, Sustainability 17(18) (2025) 8314. doi:10.3390/su17188314
[9] J. M. Ndungo, K. Rucha, Factors Affecting the Growth of SMEs: A Study of SMEs in Kajiado District. International Journal of Finance, 2(2) (2017) 58–75.
[10] L. E. Sánchez Crespo, D. Villafranca, E. Fernández-Medina, M. Piattini, Developing a Model and a Tool to Manage the Information Security in Small and Medium Enterprises, in: Int. Conf. on Security and Cryptography (SECRYPT), 2007, 355–362.
[11] L. E. Sánchez Crespo, D. Villafranca, E. Fernández-Medina, M. Piattini, Practical Application of a Security Management Maturity Model for SMEs based on Predefined Schemas, in: Int. Conf. on Security and Cryptography (SECRYPT), 2008, 391–398.
[12] S. Shevchenko, Y. Zhdanova, K. Kravchuk, Information Protection Model based on Information Security Risk Assessment for Small and Medium-Sized Business, Cybersecur. Edu. Sci. Tech. 2(14) (2021) 158–175. doi:10.28925/2663-4023.2021.14.158175
[13] S. Shevchenko, Y. Zhdanova, O. Kiia, Semi-Automated Multi-Standard Cyber Maturity Assessment Tool based on NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 and CIS Controls V8. Cybersecur. Edu. Sci. Tech. 3(31) (2025) 43–60. doi:10.28925/2663-4023.2025.31.1004
[14] H. Shevchenko, et al., Information Security Risk Analysis SWOT, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 309–317.
[15] Z. Z. F. Mthiyane, H. M. van der Poll, M. F. Tshehla, A Framework for Risk Management in Small Medium Enterprises in Developing Countries, Risks 10(9) (2022) 173. doi:10.3390/risks10090173
[16] J. F. Carías, S. Arrizabalaga, L. Labaka, J. Hernantes, Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs, IEEE Access 9 (2021) 80741–80762. doi:10.1109/ACCESS.2021.3085530
[17] M. El-Hajj, Z. A. Mirza, Protecting Small and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool, Electron. 13(19) (2024) 3910. doi:10.3390/electronics13193910
[18] M. Curtin, B. Moran, Development of a Cyber Risk Assessment Tool for Irish Small Business Owners. arXiv, 2024. doi:10.48550/arXiv.2408.16124
[19] C. Boletsis, et al., Cybersecurity for SMEs: Introducing the Human Element into Socio-Technical Cybersecurity Risk Assessment, in: 16th Int. Joint Conf. on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP), IVAPP, 2021, 266–274. doi:10.5220/0010332902660274
[20] National Institute of Standards and Technology, NIST Cybersecurity Framework Ver. 2.0 (2024). https://www.nist.gov/news-events/news/2024/02/nist-releases-draft-update-cybersecurity-framework-version-20
[21] Int. Organization for Standardization, ISO/IEC 27001: Information Security Management. https://www.iso.org/isoiec-27001-information-security.html
[22] ISACA, COBIT Framework. https://www.isaca.org/resources/cobit
[23] Center for Internet Security, CIS Controls. https://www.cisecurity.org/controls
[24] K. Al-Dosari, N. Fetais, Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach, Electron. 12(17) (2023) 3629. doi:10.3390/electronics12173629
[25] Center for Internet Security, CIS Controls v8.1 Mapping to NIST CSF 2.0 (2024). https://www.cisecurity.org/insights/white-papers/cis-controls-v8-1-mapping-to-nist-csf-2-0
[26] National Institute of Standards and Technology, NIST OLIR Program: Cybersecurity Framework v2.0 to ISO/IEC 27001:2022 Mapping (2024). https://csrc.nist.gov/projects/olir/informative-reference-catalog/details?referenceId=154

[27] ISACA, COBIT 2019 Design Toolkit for NIST CSF (2019). https://www.isaca.org/resources/toolkits/cobit-2019-design-toolkit-for-nist-csf
[28] PwC. Building cybersecurity through Top Management Cooperation, Results of the "Global Digital Trust Insights Survey 2025" for the CEE region (2025). https://www.pwc.com/ua/uk/survey/2025/cee-findings-from-the-2025-global-digital-trust-insights-survey.html
[29] V. Sokolov, et al., Adaptation of Network Traffic Routing Policy to Information Security and Network Protection Requirements, in: 13th Int. Conf. on Information Control Systems & Technologies (ICST), vol. 4048 (2025) 397–411.
[30] Y. Kostiuk, et al., Intelligent System for Simulation Modeling and Research of Information Objects, in: 1st Workshop Software Engineering and Semantic Technologies (SEST), vol. 4053 (2025) 237–251.
[31] S. Zybin, et al., Approach of the Attack Analysis to Reduce Omissions in the Risk Management, in: Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 318–328.
[32] D. Berestov, et al., Assessment of Weather Risks for Agriculture using Big Data and Industrial Internet of Things Technologies, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 1–13.
[33] D. Berestov, et al., Synthesis of the System of Iterative Dynamic Risk Assessment of Information Security, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188 (2021) 135–148.
[34] O. Partyka, A. Partyka, A. L. Imoize, AI for Web Application Security. Handbook of Cybersecurity Challenges and Solutions for Emerging Technologies (2026). doi:10.1201/9781003640790-14