Information & Security
Published since 1998

I. Tikanmäki, J. Savolainen & H. Ruoslahti
vol. 55, no. 1 (2024): 63-78
https://doi.org/10.11610/isij.5523
ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

The Role of Standards in Enhancing Cybersecurity and Business Continuity Management for Organizations

Ilkka Tikanmäki [1,2] (✉), ***Jari Savolainen,*** [1] ***and Harri Ruoslahti*** [1]

[1] *Laurea University of Applied Sciences, Espoo, Finland*
https://www.laurea.fi/en/

[2] *National Defence University, Helsinki, Finland*
https://maanpuolustuskorkeakoulu.fi/en/

ABSTRACT:

Standards are documented specifications that ensure that products, services, and systems are secure, reliable, and consistent. They unify and improve industries with requirements, recommendations, or procedures for activities or products. Standards provide information on security management systems based on industry best practices. The DYNAMO project promotes an integrated approach designed to enhance cyber situational awareness for critical sectors such as healthcare, energy, and maritime transport. This study is part of project efforts to map relevant cybersecurity standards with the research question: how can standards enhance cyber resilience?

The article presents a desktop study, including a cross-case analysis. Results show that surprisingly little is written on the practical experiences of using standards, with a lack of evidence-based experience in implementing and using standards in practice. Many benefits are presented by the standardization bodies themselves. These include compliance with legal requirements, competitive advantages, lower costs, and organisational improvements for ISO 22301. Information security professionals can use ISO/IEC 27001 to help define requirements and enhance a company's compliance and organisational improvement, and the NIST framework supports them in making informed risk management decisions while offering a high-level strategic view of an organisation's cybersecurity risk management lifecycle.

✉ Corresponding Author: ilkka.tikanmaki@laurea.fi

ARTICLE INFO:

RECEIVED: 05 SEP 2024

REVISED: 20 OCT 2024

ONLINE: 29 OCT 2024

KEYWORDS:

Cybersecurity, Business Continuity Management, Standards

Introduction

Standards and guidelines can provide a basis for cybersecurity professional development, education, and training. Project "Dynamic Resilience Assessment Method including combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors" (DYNAMO) aims to promote the ongoing enhancement and adaptability to future cyber threats through the exchange of insights and recommendations that strengthen cyber resilience[1] by combining the fields of business continuity management (BCM) and cyber threat intelligence (CTI) to create a situational awareness picture to support decision-making throughout the resilience cycle (preparation, prevention, protection, response, and recovery.[2] This approach can provide a basis for the training and education of cybersecurity professionals.

The goal of the DYNAMO project is, among other things, to investigate the effects of distractions in the critical sectors of healthcare, energy, and maritime transport[1]. Health and safety standards help reduce workplace injuries, energy management standards minimise energy consumption, and IT security standards provide security for sensitive data. This research focuses on mapping the cybersecurity standards of those sectors, why they implement standards, and what the benefits are in the development, education, and training of cybersecurity professionals.

Standards are published documents that describe specifications and procedures for ensuring that products, services, and systems are secure, reliable, and operate consistently.[3] Standards are commonly accepted and well-established regulations, guidelines, or rules developed to unify and improve an industry, a product, a service, or a process. These often identify the requirements, recommendations, or procedures that should be followed for a particular activity or product. Standards are knowledge since they are powerful tools that may stimulate innovation and enhance productivity – they can be seen as knowledge. Organisations can build success, and people's daily routine made easier and safer by using standards.[4]

This study aims to identify what benefits and challenges can be associated with the implementation of standards by examining how different organisations implement and benefit from standards such as ISO 22301 and ISO/IEC 27001 – especially what impacts standards may have on reducing risks and improving resilience. Based on the literature review, some major benefits are listed for the use of project DYNAMO, and for organisations considering the implementation of standards, such as ISO 22301 and ISO/IEC 27001.

The main research question (RQ) of this study is: How can standards enhance cyber resilience? This question is elaborated with the sub-RQ: How can standards build business continuity capabilities in organisations? The research question explores the effectiveness, challenges, and benefits of implementing cybersecurity and business continuity standards in various organisational contexts.

The article is organised into six sections: Section 1 introduces the study; Section 2 provides a literature review; and Section 3 outlines the research methodology and design. Section 4 presents the results, Section 5 discusses the findings, and Section 6 offers the conclusions.

Literature

Standards are typically based on industry best practices and can be either technical or sociotechnical. In addition, they provide information security management systems. The International Organization for Standardization (ISO) is a worldwide organisation of national standards bodies with members of 168 national standards bodies. The main cybersecurity standards reviewed in this research are ISO/IEC 27001 "Information security management systems: Requirements," ISO 22301 "Security and resilience – Business continuity management systems – Requirements" and NIST Cybersecurity Framework.

ISO/IEC 27001

ISO/IEC 27001 standard "Information security management systems: Requirements" is the international standard on information security management systems (ISMS). It is a set of standards to handle information security defining requirements ISMS must meet. Other ISO 27000 series standards support the ISO 27001 standard. Table 1 provides a brief overview of the support standards and their topics.

Table 1. Supporting 27000 series standards.

Standard number	Topic
ISO/IEC 27000	Terms and definitions used in the ISO 27k series of standards
ISO/IEC 27002	Guidelines for the implementation of controls listed in ISO 27001 Annex A
ISO/IEC 27004	Guidelines for the measurement of information security
ISO/IEC 27005	Guidelines for information security risk management
ISO/IEC 27017	Guidelines for information security in cloud environments
ISO/IEC 27018	Guidelines for the protection of privacy in cloud environments

ISO/IEC 27031	Guidelines on what to consider when developing business continuity for information and communication technologies (ICT)

The principles of ISO/IEC 27001 are confidentiality, information integrity, and availability (CIA) of information where data is protected against identified threats.[5,6] Confidentiality means that only authorised individuals are entitled to access the information, whereas integrity means that only authorised individuals may modify the information. The purpose of availability is to make data available to authorised individuals whenever required.

The second aspect is the organisational role of information system security, which is composed of a technical, social, and sociotechnical perspective.[7] The technical view focuses on technical security measures but lacks the end-user perspective. From a social perspective, technical platforms are seen as a means of communication and interaction. The sociotechnical point of view, by contrast, combines the technical and social points of view in the planning stage, but it can lead to compromises. The ISO/IEC 27001 approach to information security is by screening people, practices, and technology. An IMS implemented following this standard as a tool to manage risk, cyber resiliency, and operational excellence.[8] The main philosophy of ISO/IEC 27001 is based on the risk management process, which is to find out where the risks are and deal with them systematically with the help of security or protective measures.

ISO 22301

ISO 22301 standard "Security and resilience — Business continuity management systems – Requirements" is an international standard intended for the implementation and maintenance of effective business continuity plans, systems, and processes. The implementation and maintenance of a Business Continuity Management System (BCMS) ensures business continuity in terms of the amount and type of its effects. ISO 22301 is intended for all organisations, whether small or large, in which industry they operate or what the nature of the business is. The standard enables certification and regulatory bodies to evaluate the capacity of organisations to meet legal or regulatory requirements.[9] The objective of the ISO 22301 standard is to provide post-disruption (e.g., after natural disasters, man-made disasters, etc.) business continuity through business impact analysis and risk assessment. To avoid the above events, it is necessary to define what needs to be done and how to re-establish normal operations as soon as possible. The philosophy behind ISO 22301 is based on impact assessment and risk management by identifying the most important activities and the risks that may affect them.

National Institute of Standards and Technology (NIST)

To address cybersecurity risks, the 2014 Cybersecurity Enhancement Act (CEA) updated NIST's role to include identifying and developing cybersecurity risk frameworks for voluntary use by owners and operators of critical infrastructure.

NIST must identify “a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks.”[10]

The NIST Cybersecurity Framework is versatile even though it is designed for critical infrastructure because it enables scalability. It can be customised for any type of organisation. With its flexibility, the Framework can be used in start-up companies that launch a cybersecurity program and thereby add value to the organisation.

The core of the Framework is the common cyber security functions of the critical infrastructure, the desired results, and applicable references. Identify, Protect, Detect, Respond, and Recover are the five simultaneous and continuous functions of the Framework. The Framework has three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles.

The Framework Core consists of cyber security functions, results, and informative references common to different sectors and critical infrastructure. The Profiles of the Framework allow organizations to align and prioritize their cybersecurity activities with their business/task requirements, risk tolerance and resources. The characteristics of an organization’s cybersecurity risk management approach can be viewed and understood using the Framework’s Tiers, and thus, to prioritize and achieve the organization’s cybersecurity goals.[10]

Maritime Security Standards

There are classes on maritime security but, for example, cybersecurity is not covered with a systematic approach. Maritime standard structures are based on classifications, where standardized products are classified according to need and purpose. Cybersecurity should, therefore, be an integral component of planning and implementing, and it should encompass all aspects of the system or solution.[11] This chapter summarises the following standards: ISO/IEC 27001:2022, ISO 22301:2019 and NIST. International Maritime Organisation’s (IMO) cybersecurity-related standards for the maritime domain are listed in Table 2.

Table 2. IMO standards related to cybersecurity.

Standard number	Topic
MSC-FAL. 1/Circ.3	Guidelines on Maritime Cyber Risk Management
Resolution A.947(23)	Human element; Vision, Principles and Goals
Resolution A.647(16)	Human element; Safety Management
STCW	Human element; Training and Certification

ISO 23806:2022 “Ships and maritime technology – Cyber Safety” standard has established requirements for the identification and assessment of cyber risks and risks to the safe, environmentally responsible operation of vessels throughout their lifecycle. The standard specifies the procedural specifications that must be incorporated into a company's Safety Management System (SMS). They are also referenced to support effective cyber risk management as defined in MSC-FAL.1/Circ.3, Guidelines for Maritime Cyber Risk Management and additional requirements of the company or other identified stakeholders.[12]

Independent authorities and companies have released cybersecurity-related reports and guidelines to develop standardised continuums. Several white papers discuss common threat scenarios and risks in the marine environment. Notable maritime guidelines published by The Institute of Engineering and Technology (IET) include "Code of Practice: Cyber Security for Ports and Ports Systems" and "Code of Practice: Cyber Security for Ships."

Business Continuity Management (BCM)

BCM can be defined as the planning, preparation, and implementation of internal organisational procedures to maintain operational activities at acceptable intervals with a pre-determined capability during outages. When implementing BCM, four components should be considered: policies, processes, people, and infrastructure.[13]

Table 3. Components for implementing BCM.

Component	Topic
Policies	Organisations aims, principles and approach
Processes	Activities with defined outcomes, deliverables, and evaluation criteria
People	Roles and responsibilities
Infrastructure	Resources, technology, and equipment

The key goal of the BCM process is to analyse business impacts and design appropriate countermeasures against these. The purpose of the Business Impact Analysis (BIA) is to identify possible events that may pose a threat to business interruption. Procedures are defined based on the risk identified to prevent or mitigate the impact of events. Procedures must be tested regularly for functionality and updates. Regular and appropriate training for employees is also required. Particularly in critical sectors, cyber-attacks threaten business integrity as technology and the digitisation of enterprises are constantly evolving. Identifying adverse events and ensuring that BCM processes are in place to address them is critical.[14–16] Ruoslahti (2020) considers risk identification, critical functions, key personnel, instructions and procedures, and open communication to be important factors for continuity management.[17]

Business Continuity Management Systems (BCMS)

The purpose of BCMS is to prepare, provide and maintain controls and capabilities to manage the overall ability of an organisation to continue operating during disruptions. To achieve these, the following table presents the means intended by BCMS for organisations.[9]

Table 4. Perspectives and means for organisations (ISO, 2019).

Perspective	Means
Business	Supports strategic objectives Creates competitive advantage Protects and enhances reputation and credibility Contributes to organisational resilience
Financial	Reduces legal and financial exposure Reduces direct and indirect costs of disruption
Interested parties	Protects life, property, and environment Considers expectations of interested parties Provides confidence in the organisation's ability to succeed
Internal processes	Improves capability to remain effective during disruptions Demonstrates proactive control of risks Addresses operational vulnerabilities

When implementing BCMS, the following factors and their effects must be considered: organisational culture, involvement, resources, flexibility, and shared commitment. Building a reliable and collaborative workforce is essential to the integration of the system. Bottom-up participation in systems development is critical, as is the solicitation of input and feedback from management. Resources in the form of trained and qualified managers, supervisors, and staff are critical, and therefore, priority should be given to investing in training and ownership of the system. Flexibility in system performance should be permitted when setting up the system, and as knowledge of how it works grows, it gradually becomes more demanding. Management needs to develop an impeccable culture where learning and improvement are considered instead of difficulties and reproaches. The above factors should be included in the effective implementation of an organisation's BCM.[13, 18]

Method

This research employs a case study methodology, aiming to gain an in-depth understanding of the subject under development and to formulate recommendations for improvement. The case study research typically focuses on a single entity, frequently on a specific function or process. The qualitative case study method allows the researcher to explore various phenomena in their natural settings.[19] Analysing a case study requires data convergence through triangulation from diverse evidence sources. 'Triangulation' involves utilising various evidence sources, like data points and distinct researchers, within a single study.[20, 21] Formulating theoretical propositions in advance can be beneficial in steering the data collection and analysis procedures.[22] The research process was framed within an iterative operational model, as outlined in Yin's case study methodology.[22]

To understand the current state of research on cybersecurity and business continuity standards this study performed a desktop study of academic journals, industry reports, white papers, and official documents from standardisation organisations such as ISO and NIST (Table 5).

Table 5. Overview of type and number of analysed documents.

Type of document	n=
Academic journals	69
Industry reports	11
White papers	3
Official documents from standardisation organisations	3

The research was conducted between June 2023 and January 2024 through reading publications and documents (Table 5). The authors conducted a cross-case analysis of the data. The analysis narrows the sample by extracting data to a Data Extraction Table (DET) specifically designed for the RQs of this study.[23]

Results

This section discusses the study results, highlighting the advantages of implementing ISO standards 22301 and 27001, as well as the NIST framework. Surprisingly, the data revealed very little about the practical benefits or challenges of the reviewed standards. Mostly, the benefits were presented by the standardisation bodies themselves. This study found a clear lack of evidence-based experiences in implementing and using standards in practice.

ISO 22301 benefits

Best practices allow organisations to respond to and recover from disruptions effectively with lower costs and less impact on business performance in the event of a disruption. For companies with multiple locations or departments, the benefits are achieved with the same consistent approach across the entire organisation. Other benefits include the ability to assure customers, suppliers, regulatory authorities, and other stakeholders of stable systems and processes to ensure the continuity of operations and better business performance and resilience of organisations. The analysis of critical problems and areas of vulnerability can be considered as business development as they help better understand the entire business. Strategic planning, risk and supply chain management, business transformation, and resource management are made easier by following the principles of ISO 22301.[9] By implementing ISO 22301, a company can achieve four key commercial benefits: complying with legal requirements, obtaining a marketing advantage, reducing dependence on individuals, and preventing major losses.

Several countries have established legislation and regulations requiring BCM compliance. Private companies may also require business continuity solutions from their vendors and partners. ISO 22301 offers a framework and procedures for supporting continuity management. This means that administrative and operational efforts and possible sanctions can be reduced. Customers sensitive to business continuity in the delivery of their products and services prefer companies with ISO 22301 certified companies. Furthermore, ISO 22301 certification may enhance the organisation's reputation and help it obtain new customers. This may result in an increase in market share and profits. In many cases, the critical functions of the business are dependent on a few people who are difficult to replace. Business continuity practices provide an opportunity for managers to become less reliant on these key employees and thereby avoid many problems when somebody leaves the company. In the world of real-time services and events, every minute of unavailability is costly. While the business is not sensitive to short periods of absence, disruptive events are expensive in any case. By implementing business continuity practices that comply with ISO 22301 standard, the company obtains some sort of insurance. By preventing disruptions and recovering quickly, a business gains savings.

ISO/IEC 27001 benefits

The four key business benefits of the ISO/IEC 27001 standard are compliance with legal requirements, achieving a competitive advantage, lowering costs, and improving the organisation.[24] Obtaining an ISO/IEC 27001 certificate will show clients that their business data is protected, which, in turn, can bring competitive advantages. Preventing information security-related incidents, small and large, can save costs.[25] Fast-growing companies often seem to lack the time to define their processes and operating procedures, and implementing ISO/IEC 27001 can help address these situations by encouraging companies to record their most important processes.[26]

ISO 27001 certification protects a company's reputation by helping prevent cyber security threats to the security of information caused by, e.g., data breaches by cybercriminals or possible user mistakes made by in-house actors.[24] The benefits of ISO 27001 also include assurance that the organisation has the tools required to strengthen cybersecurity at three levels: people, processes, and technology.[26] The standard can be used to determine appropriate practices that need to be documented and protect technologies and personnel training to prevent errors. ISO 27001 assists organisations in avoiding penalties for not complying with data protection requirements like the General Data Protection Regulation (GDPR). Organisations may utilise the GDPR guidelines for obtaining and maintaining compliance. The standard's exemplary approach to information security is an appropriate starting point for multiple regulations.

The ISO/IEC 27001 Standard, however, also has challenges that need to be considered when using/implementing it: A structured approach to information and cybersecurity involves a combination of standards; Government incentives and market requirements are among the factors that motivate businesses to pursue ISO/IEC 27001 certification; the implementation process is difficult due to generic design guidelines, but there are multiple methods and levels of internalisation that can be used; there is limited evidence for certification outcomes; and the integration, motivations, implementation, and results of Information System Security (ISS) standards depend on several factors, such as the technological environment in which the organisation operates.[25, 27]

NIST benefits

The NIST Framework's five functions (Identify, Protect, Detect, Respond and Recover) support organisations in expressing their cybersecurity risk management at a high level and in making risk management decisions. The following figure illustrates these five functions of the Framework.

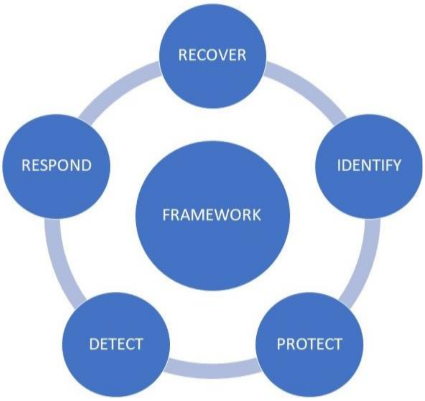

Figure 1: Five functions of the NIST Framework. Adapted from NIST.[28]

The Identify function guides an organisation in building an understanding of cybersecurity risk management for systems, individuals, assets, information, and capabilities. Resources to support critical cyber security activities and related risks enable the organisation to identify and prioritise its actions based on its risk management strategy and operational requirements. The Protect function describes the appropriate security measures for the provision of critical infrastructure services. It is used to minimise or contain the impact of a potential cybersecurity incident. The Detection function sets out the measures to detect a cyber security incident. The Detect function allows the detection of cybersecurity events on time. The Respond function includes appropriate measures in the event of a detected cybersecurity breach and supports mitigation of the effects of a potential cybersecurity breach. The Recovery function determines the appropriate measures to maintain resilience plans and restore characteristics or services compromised because of a cybersecurity breach. The Recovery function allows for a quick return to normal activities to minimise the effects of cybersecurity incidents. Together, these functions provide a high-level strategic view of an organisation's cybersecurity risk management lifecycle.[28]

Discussion

A British study of ISO/IEC 27001 in 2018 examined its benefits and basis for acquisition. The study collected data from 128 different kinds of organisations, including companies of small sizes and worldwide enterprises. The organisations that answered the questionnaire represented several branches from the private and public sectors. According to the study, the ten most popular reasons for implementing the standard were in order of importance: 1) Increasing the level of information security of an organisation, 2) Increasing competitive advantage, 3) Fulfilling laws and other mandatory requirements, 4) The nature of the industry requires implementing the best in information security practices, 5) Meeting the requirements of the EU data protection regulation, 6) As a requirement to get a new customer, 7) Committing the organisation's management to information security, 8) The evolving operating environment of cyber threats, 9) Requirement of existing customers, and 10) Costs resulting from the violation of legal requirements avoidance/demotion.[6]

The second question in the study was related to the benefits the organisations have achieved through implementation. The eight most common answers were in prioritisation order: 1) A higher level of information security, 2) Better internal processes, 3) Better information security skills of the personnel, 4) Improved company image/reputation, 5) New business partners/business opportunities, 6) Better competitiveness/higher returns, 7) Retention of existing customers, and 8) Reduction of costs resulting from data breaches. The survey gives a clear picture of what factors motivate organisations to implement an ISO/IEC 27001-compliant management system. Arguably, the biggest reason for implementation is to promote information security, which is the most important task of the standard. The second most popular reason is related to increasing the competitive advantage. Increasing competitive advantage can be seen as an economic interest which again indicates that there are also financial goals behind the implementation.[29]

Available industry and governmental directives and standards do not provide adequate covering solutions for the maritime relating to cyber-physical security, especially operational technology (OT) cyber security, even though it is recognised as critical in the overall cyber security of assets. The main body of the available standards are focusing the information technology (IT) side of the systems and operations and fails to tackle the interoperability and threats to OT systems and components in the maritime sector. The ones covering cyber-physical security are either prescriptive or based on performance and do not highlight the need for corporate policies and procedures that would apply to maritime assets onshore and offshore.[11]

Compliance with the standards, best practices, and regulations, which help minimise cyber risks, does not mean an organisation has good cybersecurity. For example, numerous ISO 27001-certified organisations tend to focus on achieving certification instead of strengthening security controls throughout their most critical information systems. This causes inconsistencies in the application of security controls in an organisation where ISO 27001-certified areas are more secure than other areas.[27]

The factors affecting the decision to obtain and maintain the certificate are divided into information security and financial benefits supplemented by additional benefits which are often closely related and overlapping. From the security point of view, the main advantage of certification is the overall increase in the security level. In finances, the certificate increases trust and sales and provides chances for cost savings. Moreover, the certificate might help cover legislative requirements such as the EU General Data Protection Regulation.[29]

Business continuity management system certification can be a heavy burden for smaller organisations compared to the benefits of certification. However, the use of the ISO 22301 standard for continuity management, even without certification, is justified because the operation following the principles of the standard enables the systematic planning, control, evaluation, and improvement of continuity management.[31]

Conclusions

Compliance with the standards, best practices, and regulations can help minimise cyber risks, so taking this into account in training can help organisations toward good cybersecurity. Best practices help organisations effectively respond to and recover from disruptions and lower impacts on business performance events of disruption. An overview of how standards can enhance cyber resilience is presented below (Table 6).

Table 6. Overview of how standards can enhance cyber resilience.

Standard	Benefits
ISO 22301	Compliance with legal requirements, competitive advantages, lower costs, and organisational improvements Best practices / Same consistent approach help respond / recover effectively and assure stakeholders of stable systems and processes Certification may enhance the reputation of the organisation
ISO/IEC 27001	Helps information security professionals define requirements

	Compliance with legal requirements Achieving a competitive advantage Lowering costs Improving the organisation
NIST	High-level strategic view of an organisation's cybersecurity risk management lifecycle Support experts in making informed risk management decisions

ISO 22301 *Security and resilience — Business continuity management systems – Requirements* (Table 6) focus on security and resilience and guide the implementation and maintenance of effective business continuity plans, systems, and processes. Some key business benefits are compliance with legal requirements, competitive advantages, lower costs, and organisational improvements. Business Continuity Management System (BCMS) provides and maintains controls and capabilities to manage the overall ability of an organisation to continue operating during disruptions (e.g., ISO, 2019). Smaller organisations may find BCM systems certification quite heavy. ISO 22301 certification may not bring direct business benefits to small companies; however, e.g., the ISO 22301 standard for continuity management is justified even without full certification. Operations that follow the principles of the standard can enable systematic planning, control, evaluation, and improvement of continuity management.[30]

The standard ISO/IEC 27001 *Information security management systems: Requirements* is the international standard on information security management systems (ISMS). Knowing the basics of this set of standards helps information security professionals define requirements that their ISMS must meet. The National Institute of Standards and Technology (NIST) framework has five functions: 1) Identify, 2) Protect, 3) Detect, 4) Respond, and 5) Recover, which help support organisation experts manage cybersecurity risks and making risk management decisions. The ISO/IEC 27001 standard provides a framework for defining ISMS requirements.[25]

Results show that familiarity with these discussed standards can aid information security professionals in managing cybersecurity risks. The National Institute of Standards and Technology (NIST) framework, for example, with its five functions—Identify, Protect, Detect, Respond, and Recover— can support experts in making informed risk management decisions.[28]

Understanding the benefits of standards and applying them to a degree relevant to the organisation in question can 1) add information security, 2) improve internal processes, 3) add company image, 4) bring new business opportunities, 5) add competitiveness, 6) retain customers, and 7) reduce of costs resulting from data breaches, and 8) mainly help improve the information security skills of the personnel.

A limitation of this study is that, surprisingly, the research question could not be fully answered with the desktop data gathered. A major finding is the lack of literature and works describing experiences gained in how standards can enhance practical cyber resilience. Results based on the sample documents show that very little has been published on practical, real-life experiences on how standards can enhance cyber resilience. Future study is recommended to gather a survey or interview data from relevant organisations on how standards can help build business continuity capabilities in organisations. Also, as results were limited to standards that have been active for some time, a further study is recommended on the effects of the newest published EU regulations.

Acknowledgement

This work was supported by the DYNAMO project, which has received funding from the European Union's Horizon Europe research and innovation funding program under the grant agreement no. 101069601.

References

[1] DYNAMO project, "Dynamic Resilience Assessment Method including combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors," 2023, https://horizon-dynamo.eu/wp-content/uploads/2023/01/DYNAMO_Leaflet_web.pdf.

[2] European Commission, *Description of the Action (DoA)*, 2022.

[3] Standards Australia Limited, "Standardisation Guide 003: Standards and Other Publications," 2019.

[4] The British Standards Institute, "Information about standards - what is a standard?" 2023.

[5] Dhillon Gurpreet and Backhouse James, "Technical opinion: Information system security management in the new millennium," *Commun ACM* 43, no. 7 (2000): 125–8, https://doi.org/10.1145/341852.341877.

[6] IT Governance UK, "Information Security & ISO 27001," 2018.

[7] Juhani Iivari and Rudy Hirschheim, "Analyzing information systems development: A comparison and analysis of eight is development approaches," *Information Systems* 21, no. 7 (1996): 551–75, https://doi.org/10.1016/S0306-4379(96)00028-2.

[8] ISO, "ISO/IEC 27001 Standard – Information Security Management Systems," 2022.

[9] ISO, "ISO 22301 — Business continuity," 2019.

[10] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 2018.

[11] Iosif Progoulakis, Paul Rohmeyer, and Nikitas Nikitakos, "Cyber Physical Systems Security for Maritime Assets," *Journal of Marine Science and Engineering* 9, no. 12 (2021): 1384, https://doi.org/10.3390/jmse9121384.

[12] ISO, "ISO 23806:2022 — Ships and marine technology — Cyber safety," 2022.

[13] Leni Sagita Riantini Supriadi and Low Sui Pheng, “Business Continuity Management (BCM),” *Business Continuity Management in Construction* (2017): 41–73, https://doi.org/10.1007/978-981-10-5487-7_3.

[14] Brahim Herbane, Dominic Elliott, and Ethné M. Swartz, “Business Continuity Management: Time for a Strategic Role?” *Long Range Planning* 37, no. 5 (2004): 435–57, https://doi.org/10.1016/j.lrp.2004.07.011.

[15] Forbes Gibb and Steven Buchanan, “A Framework for Business Continuity Management,” *International Journal of Information Management* 26, no. 2 (2006): 128–41, https://doi.org/10.1016/j.ijinfomgt.2005.11.008.

[16] Ali S. Torabi, Ramin Giahi, and Navid Sahebjamnia, “An Enhanced Risk Assessment Framework for Business Continuity Management Systems,” *Safety Science* 89 (2016): 201–18, https://doi.org/10.1016/j.ssci.2016.06.015.

[17] Harri Ruoslahti, “Business Continuity for Critical Infrastructure Operators,” *Annals of Disaster Risk Sciences: ADRS* 3, no. 1 (2020).

[18] Alan Griffith, *Integrated Management Systems for Construction: Quality, Environment and Safety*, 1st ed. (London: Routledge, 2011).

[19] Pamela Baxter and Susan Jack, “Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers,” *The Qualitative Report* 13, no. 4 (2008): 544–59, https://doi.org/10.46743/2160-3715/2008.1573.

[20] Matthew B. Miles and Michael A. Huberman, *Qualitative Data Analysis: An Expanded Sourcebook*, 2nd ed. (Sage Publications, 1994).

[21] Michael Quinn Patton, *Qualitative Research & Evaluation Methods*, 3rd ed. (Thousand Oaks, California: Sage Publications, 2002).

[22] Robert K. Yin, *Case Study Research: Design and Methods*, vol. 14, 4th ed. (Thousand Oaks, CA: Sage Publications, 2009).

[23] Norman K. Denzin and Yvonna S. Lincoln, *The SAGE Handbook of Qualitative Research*, 4th ed. (Thousand Oaks, California: Sage Publications, 2011).

[24] Luis Vilchez, “Effectiveness of ISO 27001, as an Information Security Management System: An Analytical Study of Financial Aspects,” *Far East Journal of Psychology and Business* 9, no. 3 (2012): 42–55.

[25] Giovanna Culot, Guido Nassimbeni, Matteo Podrecca, and Marco Sartor, “The ISO/IEC 27001 Information Security Management Standard: Literature Review and Theory-based Research Agenda,” *The TQM Journal* 33, no. 7 (2021): 76–105, https://doi.org/10.1108/TQM-09-2020-0202.

[26] Kyna Kosling, “5 Benefits of ISO 27001 Certification,” *IT Governance Blog,* 27th March 2024, https://www.itgovernance.eu/blog/en/benefits-of-iso-27001-certification.

[27] Sasawat Malaivongs, Supaporn Kiattisin, and Pattanaporn Chatjuthamard, "Cyber Trust Index: A Framework for Rating and Improving Cybersecurity Performance," *Applied Sciences* 12, no. 21 (2022): 11174, https://doi.org/10.3390/app122111174.

[28] National Institute of Standards and Technology, “The Five Functions,” 2018.

[29] Tatu Suhonen, "Factors that affect the decision to certify against ISO/IEC 27001 and the selection of certification body," Master's thesis, University of Jyväskylä, Jyväskylä, 2019.

[30] Mika Tanskanen, "Development of Business Continuity Management," Master's Thesis (Espoo, Finland: Laurea University of Applied Sciences, 2021).

About the Authors

Ilkka Tikanmäki (MBA in Information Systems) is a Researcher in Safety, Security, and Risk Management at Laurea University of Applied Sciences and a doctoral student of Operational Art and Tactics at the Finnish National Defence University. https://orcid.org/0000-0001-8950-5221

Jari Savolainen is a Project Specialist in safety, security, and risk management at Laurea University of Applied Sciences.

Harri Ruoslahti (PhD in Organizational communication) is a Security Management Principal lecturer at the Laurea University of Applied Sciences ResLab research team, which focuses on building resilient societal futures.
https://orcid.org/0000-0001-9726-7956