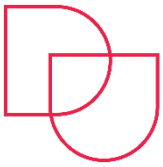


SVEUČILIŠTE U DUBROVNIKU
UNIVERSITY OF DUBROVNIK

University of Zagreb

SVEUČILIŠTE U DUBROVNIKU
EKONOMSKI FAKULTET
UNIVERSITY OF DUBROVNIK
FACULTY OF ECONOMICS
AND BUSINESS

University of Zagreb
Faculty of
Economics & Business

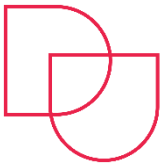
Faculty of Economics and Business Faculty of Economics & Business

Martina Schmucki

THE IMPACT OF CYBERSECURITY RISK MATURITY ON RESILIENCE: A HOLISTIC MODEL

DOCTORAL DISSERTATION

Dubrovnik and Zagreb, 2026



SVEUČILIŠTE U DUBROVNIKU
UNIVERSITY OF DUBROVNIK

University of Zagreb

SVEUČILIŠTE U DUBROVNIKU
EKONOMSKI FAKULTET
UNIVERSITY OF DUBROVNIK
FACULTY OF ECONOMICS
AND BUSINESS

University of Zagreb
Faculty of
Economics & Business

Faculty of Economics and Business Faculty of Economics & Business

Martina Schmucki

THE IMPACT OF CYBERSECURITY RISK MATURITY ON RESILIENCE: A HOLISTIC MODEL

DOCTORAL DISSERTATION

Supervisors:
Prof. Dr. Mirjana Pejić-Bach
Assoc. Prof. Dr. Josip Marić

Dubrovnik and Zagreb, 2026

SVEUČILIŠTE U DUBROVNIKU
UNIVERSITY OF DUBROVNIK

Sveučilište u Zagrebu

SVEUČILIŠTE U DUBROVNIKU
EKONOMSKI FAKULTET
UNIVERSITY OF DUBROVNIK
FACULTY OF ECONOMICS
AND BUSINESS

Sveučilište u Zagrebu
Ekonomski fakultet

Ekonomski fakultet

Ekonomski fakultet

Martina Schmucki

UTJECAJ ZRELOSTI RIZIKA KIBERNETIČKE SIGURNOSTI NA OTPORNOST: HOLISTIČKI MODEL

DOKTORSKI RAD

Mentori:
prof. dr. sc. Mirjana Pejić-Bach
izv. prof. dr. sc. Josip Marić

Dubrovnik i Zagreb, 2026.

DECLARATION OF ACADEMIC INTEGRITY

I, Martina Schmucki, declare that this doctoral dissertation, entitled "The Impact of Cybersecurity Risk Maturity on Resilience: A Holistic Model," is the result of my own original research. This research was conducted in full compliance with academic ethical standards and received formal approval from the Ethics Committee of the University of Dubrovnik (Decision Ap. no.: 1605/25), confirming the study's adherence to the principles of confidentiality, voluntary participation, and data protection. All sources of information used have been appropriately acknowledged and cited in accordance with academic standards. This dissertation has not been previously submitted for any other degree or qualification at this or any other institution.

RESEARCH COLLABORATION

This research was conducted in collaboration with the Zurich University of Applied Sciences (ZHAW), Switzerland.

INFORMATION ABOUT THE SUPERVISORS

Supervisor: Prof. Dr. Mirjana Pejić-Bach

Institution: Faculty of Economics and Business, University of Zagreb

Position: Full Professor, Department of Informatics

Mirjana Pejić-Bach received her doctorate in system dynamics modeling from the Faculty of Economics and Business at the University of Zagreb. She was trained in system dynamics at the MIT Sloan School of Management and in data mining at the Olivia Group. She is the manager and collaborator on numerous projects with Croatian companies and international organizations, especially through European Union projects and the bilateral research framework. Currently, she serves as the coordinator for the "SpinIT" project (2024–2026), focusing on smart specialization and IT spin-offs in the Danube region. Her areas of research include strategic application of information technology in business, data science, and simulation modeling. In recent years, her work has focused extensively on Generative Artificial Intelligence (GenAI), digital forensic resilience, and the AI digital divide. Her research focuses on qualitative and quantitative methodologies, particularly multivariate statistics and structural equation modeling. She is the editor of several scientific journals indexed in Scopus and Web of Science, including Business Systems Research, which she serves as Editor-in-Chief. She has won several international awards for her scientific work, such as the Emerald Literati Network Awards for Excellence. According to the Scopus database, Mirjana Pejić-Bach is among the 2% of the most-cited scientists worldwide from 2020 to 2025, as well as throughout her scientific career. She achieved the largest number of citations in the field of Artificial Intelligence & Image Processing, ranking among the top 1.35% of scientists globally in that category. A primary focus of her academic activities is mentoring doctoral candidates and developing the scientific careers of early-career researchers.

Supervisor: Assoc. Prof. Dr. Josip Marić

Institution: EM Normandie Business School, France

Position: Associate Professor

Josip Marić is an Associate Professor in Management Information Systems (MIS) and a member of the Department of Supply Chains and Digital Management at EM Normandie Business School (France). He holds a Ph.D. in management science awarded by the Université de Montpellier in 2018. As a faculty member, he is based at Paris-Clichy, and actively contributing to lectures at Caen, Dubai, Dublin, and Le Havre campuses. His pedagogical activity received *Foundation EM Normandie* award for pedagogical innovation in 2023. He serves as an Academic Director of a MSc 1st year study program running at Paris-Clichy campus. His research interests are in the areas of innovation management and Management of Information Systems (MIS), primarily focusing on the topics of digital transformation, digitalization, and the implications of digital technologies on business and society. His work is presented at various scholar conferences and events in France and abroad. At the same time, major contributions appear in internationally recognized journals such as *Technological Forecasting and Social Change*, *Technovation*, *Annals of Operations Research*, *Journal of Enterprise Information Management*, *International Journal of Logistics Research and Applications*, *Journal of Manufacturing Technology Management*, to name few.

ACKNOWLEDGEMENT

This dissertation would not have been possible without the support of many people and institutions. I am deeply grateful to my supervisor, Prof. Dr. Mirjana Pejić Bach. Throughout this doctoral journey, she provided much more than supervision. Her patience in the face of my many questions, her willingness to revisit drafts repeatedly, and the clarity she brought to moments of uncertainty made all the difference. I am equally grateful to my co-supervisor, Assoc. Prof. Dr. Josip Marić, for his careful reading and constructive comments throughout this work.

Furthermore, I extend my thanks to Andreas Grünert and Hans-Peter Käser at the Swiss National Cyber Security Centre for their significant support in defining the research goals.

My deep gratitude likewise goes to Prof. Dr. Ariane Trammell of the Zurich University of Applied Sciences, whose assistance in drafting the benchmarks significantly contributed to the quality of the survey.

I also thank my employer, Netcloud AG, for its support. In addition to providing access to survey respondents, my colleagues there provided grounded, practitioner-level perspectives on cybersecurity challenges specific to the Swiss context − insights that enriched this dissertation considerably.

Finally, I thank my family. The extensive time dedicated to a doctoral thesis inevitably tests the patience of one's loved ones. Their quiet understanding, their unwavering faith in my endeavors, and the numerous small sacrifices they made have enabled me to see this work through to the end.

SUMMARY

The increasing number and complexity of cyber threats have prompted firms globally to embrace cybersecurity as a strategic imperative. In the evolving digital landscape, an organization's capacity to recover from cyber incidents and adapt to threats is critical for maintaining operations and competitive advantage. Cybersecurity risk maturity denotes an organization’s overall capacity to detect, assess, and manage cyber risks systematically. It has emerged as a fundamental determinant of whether an organization can endure in new threat environments. Organizational resilience in cybersecurity is the ability to understand potential security threats, absorb their impact, adjust operational policies in response to these incidents, and swiftly recover, thereby ensuring operational continuity. Although the constructs of cybersecurity maturity and organizational resilience have been examined, little empirical evidence exists on how cybersecurity risk maturity affects organizational resilience.

This research addresses this gap by proposing and testing an integrated, holistic model that establishes the relationship between cybersecurity risk maturity and organizational resilience. These findings, based on structural equation modeling using data from 170 senior respondents with cybersecurity oversight at large Swiss enterprises, indicate that cybersecurity risk maturity is the primary predictor of organizational resilience, accounting for 93.4% of the variance. This refined model identifies three important pathways: the governance and leadership pathway, driven by market turbulence; the collaborative capability pathway, enabled by inter organizational engagement; and the maturity and resilience pathway, grounded in technological infrastructure and organizational capabilities.

To evaluate this relationship, a conceptual framework was developed that encompasses cybersecurity maturity models, organizational resilience theory, risk management frameworks, and dynamic capabilities perspective. The study employed quantitative research design, with a focus on structural equation modeling, and was underpinned by qualitative pilot interviews with cybersecurity professionals, including Chief Information Security Officers and senior information technology leaders, to refine and validate the research instrument for applicability across a wide range of industry and organizational settings. The theoretical model and its predicted associations were examined using structural equation modeling, multivariate analysis, and other advanced statistical techniques.

This work contributes to the literature by first presenting a robust empirical model linking cybersecurity risk maturity to organizational resilience. Second, the study finds that cybersecurity risk maturity is the foremost proximal predictor of organizational resilience, demonstrating significant predictive implications for practitioners. Third, it develops theoretical insights into enterprise cybersecurity capability strategies that support resilience amid an evolving cyber threat landscape. Fourth, this research advances applied cybersecurity research by demonstrating how structural equation modeling can empirically validate multi-level capability-governance frameworks. In practice, an organization can use the validated model to assess the maturity of its cybersecurity risk posture and select the appropriate levers to strengthen organizational resilience. The implications of this analysis support the strategic deployment of cybersecurity resources and guide investments that strengthen resilience.

The research offers recommendations for establishing governance structures and capability-building programs, and for advancing understanding of the interplay between cybersecurity and resilience. The findings inform cybersecurity governance frameworks and guide investments in continuous risk assessment. They also foster a security-aware culture and support the development of incident response systems, adaptive security architectures, and cross-functional collaboration.

The research also emphasizes leadership commitment, resource allocation, and ongoing learning, which set the stage for the maturity of organizations' cybersecurity risk management and thereby enhance resilience. Critically, the research finds that broad based awareness programs show no significant incremental effect on organizational maturity once structured training and other capability enablers are accounted for, and that market turbulence, rather than technological change alone, is the primary catalyst for organizational adaptation. The refined, evidence-based model shows that resilience evolves in a cascade: market turbulence, further amplified by rapid technological change, heightens executive perceptions of risk, prompting top management to support inter-organizational collaboration to develop the technological infrastructure and organizational capabilities necessary for mature cybersecurity risk management.

KEYWORDS

Cybersecurity Risk Maturity, Organizational Resilience, Cyber Resilience, Risk Management, Cybersecurity Governance, Maturity Models, Digital Transformation, Business Continuity

Content

1. INTRODUCTION

This chapter articulates the research problem arising from the pervasive digitalization of modern enterprises and the critical need for robust cybersecurity measures. It outlines the research objectives; the theoretical framework, which blends cybersecurity maturity models, organizational resilience theory, risk management frameworks, and dynamic capabilities perspectives; and the ten primary hypotheses developed to examine the relationships among cybersecurity risk maturity, organizational resilience, and their antecedents. Finally, the chapter summarizes the methodological approach and the anticipated scientific contributions of the dissertation.

1.1. Research problem

Pervasive digitalization has heightened the need for strong cybersecurity frameworks. However, many organizations struggle to navigate complex security protocols and to establish a coherent, strategic view of their cybersecurity posture (Sepúlveda Estay et al., 2020; Spremić, 2013). This study provides a thorough assessment of the organizational and strategic maturity of cybersecurity risk, particularly its alignment with resilience. An integral aspect of this study is the human dimension, namely, cybersecurity awareness and senior leadership commitment. Additionally, the determinants of organizational resilience are contextualized within market and technological turbulence (Durst et al., 2024). A key contribution of this study is its insights into the interrelationships among several organizational factors and their implications for the cybersecurity resilience literature. It offers an empirically grounded framework and an alternative view of cybersecurity risk maturity.

Therefore, the following research questions were formulated:

- RQ1: How do interconnected organizational, technological, and market factors drive cybersecurity risk maturity, and how does this maturity subsequently impact enterprise resilience?
- RQ2: Which technological capabilities, cybersecurity resources, human capability dimensions (awareness and training), and inter-organizational collaborative practices most significantly determine an organization's level of cybersecurity risk maturity?
- RQ3: What role do executive risk perception and top management support play in driving the collaborative and internal capabilities necessary for cybersecurity risk maturity?

- RQ4: Through which pathways do market and technological turbulence affect cybersecurity risk maturity in large enterprises, and do they act directly or indirectly via executive risk perception?

Modern cybersecurity frameworks integrate advanced technologies, such as artificial intelligence, machine learning, behavioral analytics, and automated response systems. These systems enhance an organization's ability to detect, analyze, and defend against large-scale cyberattacks (Razzaq & Shah, 2025; Lee, 2023). A recent scientometric review, spanning more than 3,700 articles, also highlighted the extensive growth of research integrating cybersecurity with machine learning and deep learning, the emergence of threat intelligence, and the need for interdisciplinary research (Razzaq & Shah, 2025). The human element is central to effective cybersecurity strategy (Moustafa et al., 2021; Pollini et al., 2022). User behavior reinforced through continuous and tailored training, is an integral component of an effective cyber defense system (He & Zhang, 2019; Chowdhury et al., 2022). A comprehensive defense and resilience policy against cyber threats will require a multidisciplinary approach that integrates technology (Panteli et al., 2025), policy (Azmi et al., 2018), and education to implement flexible strategies that accommodate the socio-technical nature of cybersecurity problems.

The main research objectives are:

1. To empirically test the structural relationship between cybersecurity risk maturity and organizational resilience in large enterprises.
2. To identify and quantify the specific technological capabilities, human resources, and collaborative practices that most significantly drive the development of cybersecurity risk maturity.
3. To evaluate the cascading governance effects of top management risk perception and executive support on the internal and collaborative capabilities required for cybersecurity risk maturity.
4. To determine how market and technological turbulence relate to executive risk perception and to cybersecurity risk maturity, and whether these environmental conditions exert direct or only indirect influence.

Rationale for selecting large companies

Several key factors support a holistic cybersecurity approach in large organizations. First, empirical analysis of over 12,000 cyber events shows that incident costs scale with firm size,

as larger revenues are significantly associated with higher absolute losses (Romanosky, 2016), while the concentration of critical assets in large enterprises makes the residual exposure strategically material. Second, the complexity of these enterprises means security must ensure alignment among technology, processes, and human behavior. Hence, performing comprehensive vulnerability assessments enables the design of tailored security controls across diverse information technology environments. Third, the concentration of intellectual property and sensitive data exposes large firms to severe reputational damage in the case of a breach (Tan et al., 2025). Fourth, the risk profile is compounded by a rapidly growing digital attack surface, caused by cloud adoption, remote work, Internet of Things networks, and third-party access (Hoffmann et al., 2020; Lee, 2023). Fifth, the transition toward Industry 4.0 entails a comprehensive re-evaluation of the workforce's capabilities to safely integrate smart manufacturing systems (Jerman et al., 2020). Finally, evidence confirms that managing these interconnected risks through mature cybersecurity governance directly affects an organization's value, stakeholder trust, and supply chain integrity (Tan et al., 2025).

1.2. Research objectives and hypotheses

This thesis examines the association between cybersecurity risk maturity and organizational resilience, offering practical guidance for enhancing security postures. It argues that businesses must invest in cybersecurity capabilities to establish sound risk maturity and resilience against complex threats.

Cybersecurity risk maturity and organizational resilience interdependence

The theoretical foundation for this relationship is derived from the dynamic capabilities' framework (Teece et al., 1997). The framework suggests that a firm's capacity to respond to environmental changes and sustain a competitive advantage hinge on its opportunity- and threat-sensing capabilities, as well as on strategic seizing of opportunities and resource allocation. These constitute the information technology security environment in which risk management capabilities enable the organization to detect threats (sensing), respond rapidly to incidents (seizing), and learn from experience to enhance future resilience (transforming). This means an organization’s cybersecurity risk management maturity covers more than just the set of technical controls; it is based on a strategic mindset of risk, embedding of business processes, and adaptive governance capacity, allowing organizations to stay ahead of the threat as it evolves and respond accordingly (National Institute of Standards and Technology (NIST), 2024; Malatji et al., 2022). Current cybersecurity resilience frameworks address dimensions

such as resistance to cyberattacks, risk management, and incident response, enabling organizations to achieve their primary objectives when affected by cyberattacks, as reported by the NIST (2024). In this research model, cybersecurity risk maturity plays a central mediating role, directly affecting organizational resilience, which constitutes the primary hypothesis. The maturity of cybersecurity risk management influences organizational resilience (Sepúlveda Estay et al., 2020; Malatji et al., 2022). This represents a proactive capability to assess cyber threats and predict future attacks through risk assessment and threat intelligence (Lee, 2023; Razzaq & Shah, 2025). Moreover, it enables an organization to resist attacks effectively, as the business model is designed to manage cyber threats. In addition, such an organization demonstrates operational effectiveness in incident response, with strong incident management practices and business continuity plans that can be rapidly adjusted during a cyber breach (Business Continuity Institute, 2024; Elliott & Swartz, 2010).

According to Ahmad et al. (2020), integrating information security management and incident response functions enables both single-loop and double-loop organizational learning, allowing an organization's cyber defense to evolve in response to new threats or technologies. Previous literature on organizational cyber-resilience argues that cybersecurity should be integrated into the broader strategic planning system, not only to maintain resilience but also to address situations in which environmental volatility and sensitive economic conditions coexist (Järveläinen et al., 2025). Therefore, organizations need to consider cybersecurity programs a key capability for protecting brand value, maintaining regulatory compliance, and securing a competitive position in increasingly digitized markets, where cyber incidents can have significant consequences for stakeholder relationships, such as with customers (Tan et al., 2025). They should also understand the interrelationship between an organization's cybersecurity risk maturity and resilience. This enables organizations not only to respond adequately to cyber incidents but also to respond more quickly and effectively when problems arise, thereby preserving their longevity and future success. Therefore, the following hypothesis is proposed:

- H1: Higher cybersecurity risk maturity positively impacts organizational resilience

Technological infrastructure and cybersecurity risk maturity interdependence

Cybersecurity risk maturity encompasses the formalization and optimization of policies, processes, and technologies that collectively strengthen an organization's security posture (Brezavšček & Baggia, 2025; Aliyu et al., 2020). Technological infrastructure refers to vast

networks of computing and communication systems, storage technologies, and data and software that enable modern economies (Kilani, 2020). As Internet of Things technologies expand into cloud and edge computing, the current technology landscape has upended the status quo in technical architecture and security solutions, and introduced new paradigms for distributed security administration, identity federation, and cross-platform threat identification (Lee, 2023). This architectural shift is reflected in a broad-based shift in security paradigms from perimeter-based models to zero-trust architectures, in which no implicit trust is assumed within organizational networks. New security architectures need to underpin the distribution, dynamism, and heterogeneity of the technological environment while ensuring the coherent, consistent application of their policies and controls (NIST, 2024). The complementarity between these two dimensions is essential for safeguarding digital infrastructure and ensuring the digital system's resilience against cyberattacks. In fact, Kilani (2020) demonstrates that infrastructure mediates the relationship between cybersecurity motivators and organizational internal processes, suggesting that while technology enables efficiency and scalability, it simultaneously creates attack surfaces that require mature risk management.

Cybersecurity risk maturity growth relies on the continuous analysis of the underlying technical architecture. In addition, the evolving dynamics of cyber threats necessitate continuous updates and refinement of protective measures. The focus on "security by design" (Geismann et al., 2018) is critical because new technologies must be designed with security considerations embedded from inception. Current research confirms that technology-centric cybersecurity must also account for the human dimension. Panteli et al. (2025) argue that responsible cybersecurity requires a multi-layered approach encompassing techno-centric, human-centric, and organizational dimensions. Complementarily, Pollini et al. (2022) demonstrate that integrating human factors engineering with cybersecurity frameworks, including user-centered design principles—significantly improves security outcomes. With this in place, the infrastructure ecosystem becomes more resilient to a broader range of cyberattacks. However, the relationship between technology infrastructure and cybersecurity risk maturity remains complex and requires ongoing investigation. Consequently, the following hypothesis is proposed:

- H2a: A more developed technological infrastructure positively impacts cybersecurity risk maturity

Cybersecurity resources and capabilities, and cybersecurity risk maturity interdependence

Modern cybersecurity resources and capabilities can include human, technological, and financial resources, as well as institutional processes, requirements, and controls necessary to implement cybersecurity effectively. This encompasses personnel with cybersecurity skills, technology-based security products, threat intelligence feeds, incident response capabilities, and continuous learning frameworks (NIST, 2024; (ISC)², 2023). There is a severe global shortage of cybersecurity personnel, with approximately 4 million unfilled positions worldwide. For organizations seeking to cultivate internal cybersecurity expertise, identifying and retaining individuals best suited for these roles is a significant challenge, necessitating holistic workforce development strategies that offer multiple pathways to entry, career development, and retention interventions ((ISC)², 2023).

Cyber risk maturity refers to the extent to which an organization can effectively manage and control these risks within its overall risk management strategy, rather than treating them as a standalone strategic priority. The relationship among these components ultimately rests on the premise that cyber threats are dynamic. New vulnerabilities are emerging, and threat actors are becoming more sophisticated (Verma et al., 2025). Investing in cybersecurity without continuous capability development and dynamic resource allocation could result in substantial capital expenditures. As Linkov and Kott (2018) indicate, during cyber storms, organizations must foster a learning environment; otherwise, they cannot pivot and adapt their strategies quickly enough to counter evolving threats. The maturity of cyber risk management is closely linked to cybersecurity resources and capabilities, which, in turn, require a governance structure that aligns them with the company's objectives (Hoffmann et al., 2020). An important part of cybersecurity governance in the modern era is board-level awareness, senior management commitment, and transparent accountability, which enable efficient resource allocation and ensure that strategic objectives align with broader organizational risk management principles. This approach aims to ensure that organizational objectives align with continuous management goals (Burch et al., 2024). This relationship underpins a proactive cybersecurity posture, leading to the following hypothesis:

- H2b: More developed cybersecurity resources and capabilities positively impact cybersecurity risk maturity

Cybersecurity awareness and cybersecurity risk maturity interdependence

Cybersecurity awareness in this research refers to cognitive and cultural factors in the cyber domain: employees' foundational knowledge, perceptions, and understanding of threats, vulnerabilities, and defensive mechanisms within their specific domains. This includes skills in threat identification, secure behavior, and the seamless integration of cybersecurity considerations into daily work tasks. A human-centered perspective on modern cybersecurity acknowledges that success relies heavily on people's behavior, choices, and culture, as well as on technological solutions. Panteli et al. (2025) argue that responsible cybersecurity requires attention to the human-centric layer, which encompasses user-centered system design and the welfare of security professionals. The focus of cyber awareness programs is to increase a person's knowledge of cyber risks, the behaviors needed to minimize risk, and how to recognize phishing emails and protect sensitive information. Human factors remain the most volatile variable in the cybersecurity equation, often bypassing even the most sophisticated technical controls (Ebert et al., 2025). Cybersecurity awareness programs are the basic building blocks of a security culture in which employees play an active role in cyber defense (Alshaikh, 2020; Arbanas et al., 2021) and should be evaluated using regular metrics on impact, sustainability, accessibility, and monitoring (Chaudhary et al., 2022). However, the true effect of such programs depends primarily on whether they can induce and sustain changes in employees' work behavior, requiring an evidence-based design.

Cybersecurity awareness is congruent with cybersecurity risk maturity. Increased attention to information security enables organizations to better prevent incidents and address them. This maturity is based on the organization-wide adoption of a thorough understanding of cybersecurity policies, procedures, and best practices, developed through effective awareness programs. Modern cybersecurity training and awareness campaigns now go beyond traditional compliance-based security education to incorporate behavioral change theories, adult learning principles and cultural sensitivity that can ensure sustainable appropriation of secure practices; empirical evidence shows that to be effective, cybersecurity education requires continuous repetition, personalized content, and integration into the values of an organization rather than one-time training events or generic awareness materials (He & Zhang, 2019; Chowdhury et al., 2022).

Organizations that invest in continuous, diversified, and comprehensive cybersecurity education programs are better positioned to mitigate human error, a major contributing factor

to cybersecurity attacks (Jeong et al., 2019; Pollini et al., 2022). The relationship between cybersecurity awareness and cybersecurity risk maturity is fundamental to cybersecurity management. Enhancing awareness programs within an organization is not merely a compliance activity; it is a strategic requirement that contributes to overall cyber hygiene. Therefore, the following hypothesis is formed:

- H3a: Higher cybersecurity awareness positively impacts cybersecurity risk maturity

Security training and cybersecurity risk maturity interdependence

Cybersecurity training initiatives are central to developing and enhancing an organization's cybersecurity risk maturity. In this study, cybersecurity training is defined as formal professional learning activities, structured curricula, and competency development programs to build employees' knowledge, perception, and understanding of cybersecurity threats, vulnerabilities, defensive mechanisms, and preventive practices. Training includes skill development in threat identification, the formation of secure behavior (also known as safe requisite behavior), and the integration of cybersecurity considerations into daily work activities (Chowdhury et al., 2022; Hatzivasilis et al., 2020). Recent research suggests that training platforms should be well-designed to facilitate adoption and ensure that security practitioners are comfortable and supported in applying cybersecurity practices (Hatzivasilis et al., 2020; Chowdhury et al., 2022). The purpose of cybersecurity training programs is to build structured competencies and formalized practices that translate employee knowledge into measurable cybersecurity risk maturity. According to Chaudhary et al. (2022), a security-oriented culture is essential to organizational resilience, as targeted training initiatives position employees as active participants in cyber defense. This aligns with Alshaikh (2020), who demonstrates that cultivating a robust cybersecurity culture effectively shapes employee behavior, making them proactive participants in organizational protection.

The effectiveness of cybersecurity training programs is inextricably linked to their ability to foster sustained behavior change among employees; therefore, their design and implementation require an evidence-based approach. Practical cybersecurity training directly develops and strengthens cybersecurity risk maturity by institutionalizing skill-based security practices across the organization. Formalized training is the foundation on which employees adopt, apply, and consistently follow the policies and procedures that constitute mature risk management. Organizations that implement comprehensive, ongoing cybersecurity training become more resilient against cybercrime, as such training helps prevent human error, a leading cause of

cybersecurity incidents (Jeong et al., 2019). Cybersecurity management is grounded on the fundamental concept of structured, formal training programs that build measurable competencies and support systematic risk lifecycle practices. Hence, the following hypothesis is generated:

- H3b: Higher cybersecurity training positively impacts cybersecurity risk maturity

Cybersecurity alliance & collaboration, and technological infrastructure interdependence

Contemporary cybersecurity alliances encompass numerous forms of cooperation, information-sharing, and mutual defense mechanisms, as well as the capacity for organizations to leverage intelligence, assets, and skills to enhance cyber defense through coordinated efforts—from public-private partnerships and industry consortia to threat intelligence-sharing platforms and cross-sector cooperation. Here, cybersecurity alliances and partnerships are paramount. They develop unified security processes and guidelines to ensure interoperability and defend against security vulnerabilities (Lee, 2023). In addition, collaborations enable rapid responses to cyber challenges. Consequently, members can mobilize pooled resources to respond rapidly to cyberattacks, thereby mitigating damage. In cybersecurity, the convergence of technology, human guidance, and regulatory frameworks has become a key factor in building resilience in the digital landscape; recent literature suggests that cybersecurity alliances, particularly through Information Sharing and Analysis Centers (ISACs), provide opportunities for joint capacity development through common training programs, exercises, and research (European Union Agency for Network and Information Security, 2018). Driven by innovation, education, and policy reform, cybersecurity alliances provide an essential defense mechanism, strengthening the technological infrastructure that protects organizations from cyber threats. Therefore, the following hypothesis is formed:

- H4a: A more developed security alliance and collaboration positively impact technological infrastructure

Cybersecurity alliance & collaboration, and cybersecurity resources and capabilities interdependence

The alignment of resources and capabilities in cybersecurity alliances is the main factor in success. With advanced threat monitoring, rapid recovery strategies, and full-scale restoration measures (Lee, 2023), the sharing and use of heterogeneous resources enhance resilience. The cooperative character of cybersecurity alliances enables joint capability improvement, as

partners can enhance defensive and offensive capabilities through cooperation on training, exercises, and R&D projects, which is critical for addressing a dynamic threat environment that evolves faster than traditional policymaking. It is this common multiplication of capabilities that is critical to confronting the rapidly evolving cyber threat environment (which, in many places, can escalate at a pace that outpaces the traditional linear pace of policy and strategy development). However, the challenge of converging the resources and capabilities of cybersecurity alliances is daunting.

Effective cooperation in cybersecurity alliances requires flexible, forward-looking approaches to address rapidly changing threats (Järveläinen et al., 2025), encompassing shared risk capacities and long-term stakeholder commitments to privacy and confidentiality. Cybersecurity awareness is vital to joint efforts to ensure the safety of cyberspace, which encompasses the interconnectedness of cybersecurity partnerships and cooperation. This research yields the following hypothesis:

- H4b: Improved collaboration and security alliance has a positive effect on cybersecurity resources and capabilities

Cybersecurity alliance & collaboration and cybersecurity awareness interdependence

Cybersecurity alliance and collaboration have a complex relationship with awareness. The alliances provide a forum for sharing the most up-to-date information on cyber threats, which can then be integrated into training programs, making them current and relevant. This strengthens the knowledge profiles of all employees and stakeholders and promotes a proactive cybersecurity policy within organizations (Glaspie & Karwowski, 2018; Alshaikh, 2020). Moreover, through joint efforts, they can contribute resources to developing well-rounded training content and programming that an individual institution might not be able to afford or manage. These resources can be shared among alliance participants to enable widespread access to high-quality cybersecurity training and awareness programs. In executing cybersecurity awareness initiatives, alliances and partnerships draw on a range of tools and tactics to ensure effective communication and participation. Such opportunities may take the form of workshops, seminars, web-based courses, and simulations that emulate real-world attacks.

In the realm of cybersecurity alliances and awareness, academic research on their relationship reveals a recurring theme: informed stakeholders significantly enhance the effectiveness of cybersecurity strategies. A study by Li et al. (2019) found a positive association between

cybersecurity policy awareness and employees' cybersecurity behavior. This discovery underscores the essential role of awareness and education in cybersecurity and provides evidence that alliances do invest in these arenas. However, there are also challenges to note in this interrelatedness. Threats to cyber life are dynamic; therefore, cybersecurity alliances and awareness campaigns must be adaptive and foresight oriented. Key challenges include scaling awareness programs to meet diverse audience needs, engaging stakeholders, securing shared intelligence, and managing privacy and confidentiality concerns. Cybersecurity alliances play a significant role in collaboration and cybersecurity awareness, serving as collective strategies to protect cyberspace. With coordinated partnerships and targeted awareness initiatives, cybersecurity can adapt and respond to the diverse threats it faces across clients and systems. Hence, the hypothesis based on the aforementioned research is:

- H5a: A more developed security alliance and collaboration positively impact cybersecurity awareness

Cybersecurity alliance & collaboration and cybersecurity training interdependence

The roles of cybersecurity training and strategic partnerships are crucial. Today, human factors remain one of the most significant cybersecurity weaknesses. This means that extensive, continuous training programs are vital for preparing individuals and personnel to recognize cyber threats and apply the necessary skills to mitigate them (Alshaikh, 2020; Glaspie & Karwowski, 2018). Current cybersecurity training models within alliances illustrate this with improved effectiveness through organized methods that engage individuals and organizations' collective knowledge and resources, allowing alliance members to benefit from specialized training programs, threat intelligence updates, and collaborative learning opportunities that would prove challenging to develop independently (Neri et al., 2025; Cybersecurity and Infrastructure Security Agency (CISA), 2023a). Cybersecurity information-sharing alliances can improve insight into threats and incidents, while broad training initiatives can strengthen employees' security awareness (Fransen et al., 2015; He & Zhang, 2019; Chowdhury et al., 2022). Cybersecurity alliances and training can significantly enhance one another, thereby strengthening cyber resilience. Alliances, to an extent, promote and facilitate access to cybersecurity training programs within member organizations and recognize that the human element is central to their security strategy. On the other hand, well-informed individuals who receive concurrent training work effectively together in cybersecurity by adhering to security frameworks and sound cyber practices. The dynamics of this interconnection warrant further

investigation, particularly in the context of the evolving cyber threat landscape and the development of new cybersecurity technologies and applications. Based on the previous studies, it is hypothesized:

- H5b: A more developed cybersecurity alliance and collaboration positively impact cybersecurity training

Cybersecurity top management support and cybersecurity alliance & collaboration interdependence

Top management support for the formulation and implementation of cybersecurity strategies is critical. The commitment and involvement of senior leadership not only provide financial resources for the effort but also underscore the importance of such policies within the organization. This requires board-level oversight of cybersecurity governance. However, precise accountability is essential, particularly at the governance level, where the principal-agent relationship must ensure that cybersecurity professionals align with the organization's strategic objectives and that resources are allocated appropriately (Burch et al., 2024). Top management support for cybersecurity refers to the commitment of time, energy, and guidance from senior executives and the board of directors to ensure the organization's corporate cybersecurity capability. This construct aligns with the governance perspective in agency theory, in which principals (board members) must actively oversee and direct cybersecurity activities to prevent interest misalignment (Burch et al., 2024). The responsibility of top management is to establish a culture of cyber resilience, drive compliance, and treat cybersecurity as a strategic imperative. Thus, the symbiosis between top management endorsement and cybersecurity partnerships is mutually beneficial. Organizations considered mature in cybersecurity are often motivated to collaborate on shared security initiatives to increase their use of shared resources and intelligence networks. In contrast, participation in cybersecurity alliances underscores the strategic importance of cybersecurity to senior leadership by providing tools to understand the constantly evolving threat landscape and to justify ongoing investment in cybersecurity defenses.

Providing appropriate financial and human resources is key to advancing cyber risk maturity and resilience (ISACA, 2022). Organizations must make strategic investments in cybersecurity technologies, personnel, and training to develop and maintain a robust defense system. The Gordon-Loeb model provides a framework for determining optimal investment levels, demonstrating that cybersecurity spending should be calibrated to expected losses and

vulnerability levels rather than applied indiscriminately (Gordon et al., 2016). The cybersecurity budget should be aligned with an organization's risk appetite and strategic objectives. Many organizations find it difficult to justify such expenditure because their business priorities conflict (ISACA, 2022; Gordon et al., 2016). Risk quantification frameworks, such as the Factor Analysis of Information Risk (FAIR), can translate cybersecurity risks into financial terms and support informed investment decisions (Freund & Jones, 2014; FAIR Institute, 2024). Furthermore, top management support for participation in cybersecurity alliances aligns the organization with the ecosystem, strengthens resilience to cyber threats, and establishes a culture of cyber resilience at both the individual and organizational levels, thereby making the joint defense mechanism adaptive and robust (Neri et al., 2025). Organizations with stronger top-management support have improved access to strategic roles in cybersecurity alliances, and leadership buy-in helps allocate resources across the organization to support collaborative security work and the sharing of intelligence. Therefore, the following hypothesis is defined:

- H6: Higher cybersecurity top management support positively influences cybersecurity alliance and collaboration

Cybersecurity top management risk perception and cybersecurity top management support interdependence

Evidence supports a link between top management's cybersecurity risk perception and their cybersecurity support, showing that organizational leadership's risk perceptions significantly affect resource allocation and the strategic direction of cybersecurity-related activities. According to Al-Sartawi (2020), top management support is vital to the planning and implementation of cybersecurity strategies; its involvement and dedication not only provide financial strength but also signal the value of cybersecurity policies within the organization. Cybersecurity Top Management Risk Perception is the expert judgment and cognitive appraisal of cybersecurity threats and vulnerabilities used by top management, and its influence on organizational objectives and stakeholder value. This concept is derived from Sonnenschein et al.'s (2017) model of top managers' security awareness (identifying individual knowledge, attitudes, and perceived responsibility) and from the agency-theory perspective on governance accountability presented by Burch et al. (2024). The sophistication of cyberattacks, their delivery via ransomware and supply chain compromises, and recent advances in advanced persistent threats are making cybersecurity a board-level concern (Tan et al., 2025),

necessitating strategic planning, resource allocation, and risk management. At the pinnacle of any organization, this not only drives how senior executives view these threats but also determines where they allocate their investment in protective technologies, human resources, and training programs. It is also important to note that leaders who understand the risks associated with cyberattacks are more likely to design stronger security capabilities.

Cyber incidents can significantly diminish brand value and stakeholder trust, necessitating robust cybersecurity programs to meet regulatory standards and remain competitive (Tan et al., 2025). Organizations' assessment of their cybersecurity risk from the perspective of upper management is intrinsically correlated with their adoption of cybersecurity practices, which, in turn, depends to some extent on the creation and acceptance of effective security postures within the organizations. This interconnectedness highlights the significance of developing informed and knowledgeable leadership in a heterogeneous cyber threat context, and thus leads to the hypothesis as follows:

- H7: Higher cybersecurity top management risk perception positively influences cybersecurity top management support

Market turbulence and cybersecurity top management risk perception interdependence

Central to this relationship is that market turbulence increases senior management's perception of risk. Notably, market fluctuations create environmental uncertainty, which heightens management's awareness of perceived threats, particularly cyber threats (Durst et al., 2024). Market turbulence is a dynamic environmental condition characterized by rapid changes in customer behavior, competitive landscapes, regulatory requirements, and economic conditions that engender uncertainty and require organizations to pivot (Durst et al., 2024; Jaworski & Kohli, 1993). Current market volatility is driven by digitalization and globalization, regulations such as the GDPR and Switzerland's data protection laws, and by new technologies that offer opportunities as well as cybersecurity risks (Federal Council, 2023). A more uncertain market, where uncertainty is the norm and ambiguity shapes risk awareness, is likely to lead managers to greater vigilance and attention to holistic risk assessment approaches, as articulated in frameworks such as the COSO ERM Framework (Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017) and the NIST Cybersecurity Framework (NIST, 2024).

Market turbulence generates volatile environmental conditions that prompt adaptive organizational responses, particularly in risk management (Durst et al., 2024). The change is not limited to economic factors; it also entails greater compliance with regulatory authorities. During turbulent markets, executives become hyper-focused on common risks across all business areas, cybersecurity, for instance, because volatility tends to magnify both the threat and the anticipation of cyberattacks. The fact that cyberattacks during market uncertainty exacerbate negative impacts on business performance and stakeholder confidence further underscores the need for firms to embed cybersecurity considerations and policies into strategic planning to remain resilient against cyberattacks (Järveläinen et al., 2025).

Recent studies indicate that environmental uncertainty increases risk perceptions by broadening decision-makers' consideration of potential threats and their interrelationships, particularly amid pressure from digital transformation and regulatory compliance mandates (Durst et al., 2024). Increased awareness stems from the realization that cyberattacks during market turbulence can further exacerbate adverse organizational outcomes and raise costs, necessitating improved risk assessment processes (COSO, 2017). Moreover, top management's perception of cybersecurity risk during market turbulence strongly influences their increased investment in cybersecurity. Such risk perception becomes salient and emergent in an industry where markets continue to evolve, and customer preferences, competitive conditions, and regulatory expectations frequently change (Durst et al., 2024; Jaworski & Kohli, 1993). Such a relationship underscores that when organizations face environmental pressures, cybersecurity must be integrated into strategic planning to ensure resilience, a cornerstone of national cybersecurity strategies (Federal Council, 2023). Academic literature suggests that market turbulence is an environmental signal and may also enhance management's cognitive attention to risk drivers within the organization. Swiss firms operating in turbulent markets subject to international compliance obligations require stronger awareness and risk-management capabilities (Federal Council, 2023).

Consistent with a positive increase in risk awareness observed during market turbulence and top management's perception of cybersecurity risk (Durst et al., 2024), the relationship indicates that environmental uncertainty has a positive multiplier effect on risk awareness, thereby facilitating the development of risk-control maturity. Integrating cybersecurity risk management with overarching strategic planning during crises demonstrates increased risk awareness and alignment with national cybersecurity policies and best practices worldwide (Federal Council, 2023; NIST, 2024). In this way, market turbulence itself induces heightened

risk perception, which, in turn, can promote better risk management and organizational resilience. The relationship between market turbulence and top management's perception of cybersecurity risk implies a positive amplification effect: environmental uncertainty enhances risk consciousness rather than reduces it; as such, it underlies well-established risk management features (COSO, 2017; International Organization for Standardization (ISO), 2022a). Therefore, the research described above is the crystallization of the following hypothesis:

- H8: Cybersecurity top management risk perception is positively affected by higher market turbulence

Technological turbulence and market turbulence interdependence

Recognizing that technological advancements shape market dynamics is central to understanding the interplay between technological and market turbulence (Durst et al., 2024). Technological turbulence refers to rapid technological change and obsolescence within an industry (Durst et al., 2024). Present-day technological changes, including artificial intelligence, cloud computing, the Internet of Things, and the emergence of quantum computing, demonstrate such turbulence and require sophisticated strategies to identify and mitigate cybersecurity risks (Dal Cin et al., 2025; NIST, 2024). Technological transformation takes place so quickly that an environment where the uncertainty and complexity are constantly rising demands organizations to continue to reassess their strategy orientations and redraft their objectives as technological shocks create instability in the market, including the introduction of new competition dynamics and customer demands, and the modification of industry structures (Järveläinen et al., 2025). Technological disruption tends to trigger market instability by establishing new competitive paradigms, altering customer expectations, and restructuring industries. Flexibility in managing technological disruptions is a great indicator of organizational agility in the digital age (Durst et al., 2024).

Technological turbulence refers to the rapid, unpredictable evolution of technology that can create new threats and opportunities for cyberattacks (Durst et al., 2024). Organizations need to build the capacity to monitor the future technology horizon, assess the implications of emerging technologies, and implement targeted cybersecurity improvements (Dal Cin et al., 2025). It requires a culture of continuous learning and innovation, as well as the ability to adopt new technologies and practices as needed (NIST, 2024). The ability to respond to technological turbulence is crucial to an organization's mature, resilient cybersecurity posture (CISA, 2023a). In contrast, market turbulence is reflected in customer preferences, competitive actions,

regulatory landscapes, and broader socio-economic changes (Durst et al., 2024). As technology evolves, new forms of competition alter the market's dynamics and boundaries. According to innovation theory and the disruptive nature of technological change, technological innovations disrupt established market structures and open up different opportunities and challenges to organizations operating within these market conditions, consistent with the interplay between technological and market turbulences, in part because technology creates (or disrupts) the existing market structure by changing the way businesses are organized. Technological change interacts with market uncertainty, as technological discontinuities can trigger periods of turbulence characterized by intense competition among technological designs, ultimately reshaping industry structures (Tushman & Anderson, 1986). This dynamic forces organizations to adapt their strategies to both technological and market changes simultaneously (Durst et al., 2024). Thus, the following hypothesis is proposed:

- H9: Greater technological turbulence has a positive effect on market turbulence

Technological turbulence and cybersecurity risk maturity interdependence

Technology disturbances are rapid changes that challenge established risk management practices (Durst et al., 2024; Tushman & Anderson, 1986). Rapid technological change introduces numerous new vulnerabilities, attack vectors, and security problems that can outpace existing risk management capabilities (Cheimonidis & Rantos, 2023; Kaur & Ramkumar, 2022). High technological instability impedes effective risk evaluation and response, making it challenging to maintain a robust security posture (Cheimonidis & Rantos, 2023; Rajasekharaiah et al., 2020). This strain on resources is a key factor, as organizations must make difficult resource allocation decisions between investing in new technologies to remain competitive and investing in the security measures needed to protect them, which can negatively impact the maturity of their cybersecurity risk management (Gordon & Loeb, 2002; Gordon et al., 2016).

Organizations need to build adaptive risk management structures that can keep pace with technological change and maintain coverage of emerging threats and known vulnerabilities. This equilibrium can be attained only through complex risk-control measures that accommodate evolving technological environments while maintaining consistent security practices. Disruptive technological innovation can also pose issues for how companies allocate capital: for instance, they may have to invest in new technology, yet the same security measures that help keep it secure can increase costs (Christensen, 1997). This dual investment can strain resources, potentially leading to a less mature cybersecurity risk management posture.

Therefore, businesses require adaptive, dynamic risk management models that evolve with the technological environment to effectively address emerging threats and vulnerabilities (Cheimonidis & Rantos, 2023; Hoffmann et al., 2020). Thus, the underlying hypothesis is defined as follows:

- H10: Greater technological turbulence negatively affects cybersecurity risk maturity

Research model integration

The hypotheses are framed within an integrated theoretical model that examines the intricate relationships among organizational factors, environmental turbulence, and cybersecurity outcomes. The model is inspired by contemporary cybersecurity research that highlights the socio-technical nature of the threat landscape and calls for an integrative approach encompassing technological, human, and organizational dimensions (Panteli et al., 2025). It identifies cybersecurity risk maturity as a central mediating variable in the determinants of organizational resilience, influenced by numerous integrated internal organizational and exogenous environmental variables (Durst et al., 2024). As organizations' focus on cybersecurity capacity development in complex and dynamic environments grows, they need to consider cybersecurity through multiple theoretical lenses. Järveläinen et al. (2025) highlight the importance of integrating dynamic capabilities and collective mindfulness for critical infrastructure resilience, and Panteli et al. (2025) support a socio-technical perspective that encompasses technological, human, and organizational aspects. This integrated model contributes to the literature by treating cybersecurity as a strategic organizational capability rather than a technical function, an important consideration in cybersecurity investment frameworks, governance structures, and capability development initiatives (Durst et al., 2024; Järveläinen et al., 2025).

1.3. Sources and methods of research

The doctoral thesis consists of theoretical and empirical sections. It utilizes both primary and secondary data sources. The survey employs a seven-point Likert-scale questionnaire as the primary data-collection instrument. The theoretical portion of the thesis, based on secondary sources, reviews Swiss and international scientific literature to elucidate contemporary knowledge and research. A pilot study was conducted to assess the questionnaire's validity and comprehension. The questionnaire was used to conduct the primary survey. Surveys were distributed via email, with a link to a Google Docs form. Reminders were sent to collect the

required number of questionnaires. The target population comprised board members, cybersecurity leaders, IT managers, and other relevant professionals with knowledge and experience in cybersecurity governance. Participants were assured of data anonymization and confidentiality.

Statistical analysis

There were four phases in data analysis. First, the sample parameters for a demographic concern analysis are determined. Descriptive statistics are used to analyze this information. Second, the manifest variables are analyzed with descriptive statistics. The average, standard deviation, and coefficient of variation of each manifest variable are calculated, and the manifest variable entries are presented in graphic form. Thirdly, the validity of the research instrument is examined with confirmatory analysis. Confirmatory factor analysis is used to evaluate the validity of the measurement model and its latent constructs. The analysis is conducted on the following latent constructs: Resilience (R), Cybersecurity Risk Maturity (CSRM), Technological Infrastructure (TI), Cybersecurity Resources & Capabilities (CSRC), Cybersecurity Awareness (CSA), Cybersecurity Training (CST), Cybersecurity Alliance and Collaboration (CSAC), Cybersecurity Top Management Support (CSTMS), Cybersecurity Top Management Risk Perception (CSTMRP), Market Turbulences (MT), Technological Turbulence (TT). Factor loadings will be computed for all manifest variables, and indicators with loadings below 0.4 were excluded from the analysis.

The dissertation is further supported by Structural Equation Modeling (SEM), which validates the hypotheses formulated herein. The comparative fit index (CFI), root mean square error of approximation (RMSEA), and standardized root mean square residual (SRMR) indices are used to assess the goodness of fit of the SEM model. SEM modeling will provide regression equations in which latent variables serve as both dependent and independent variables. Acceptance or rejection of the hypothesis will be determined by the statistical significance of the estimated parameter at the 5% level; coefficients significant only at the 10% level are reported as marginal and are not treated as confirmatory support. The structural equation model under consideration is shown in Figure 1.

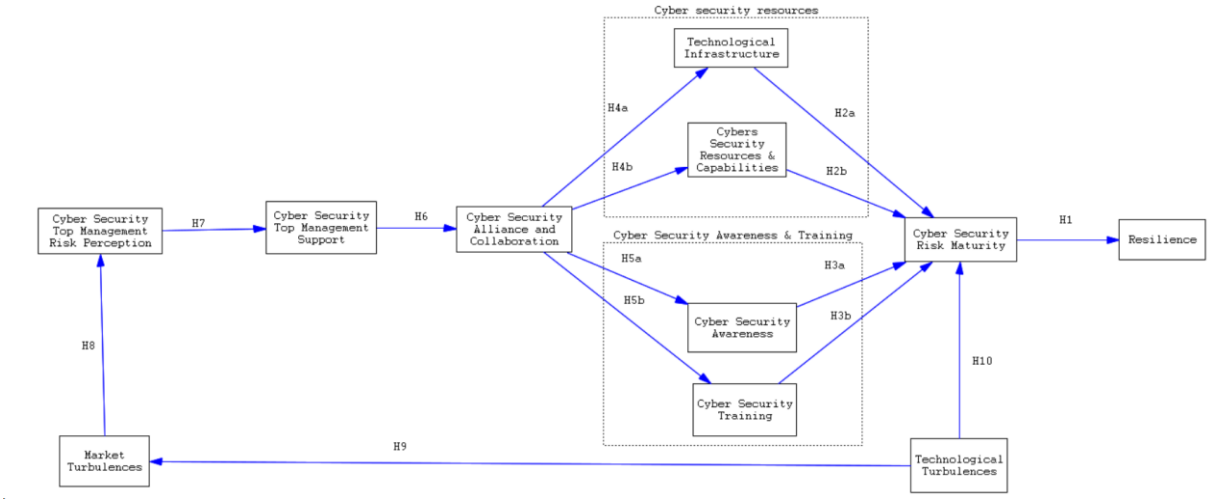


Figure 1: Research model

Source: Author's work

The model in Figure 1 integrates organizational, technological, and governance-related determinants to explain differences in cybersecurity risk maturity and, ultimately, organizational resilience. The hypotheses specify both direct effects and a cascading set of relationships: top management's risk perception and support enable alliance and collaboration, which, in turn, strengthen internal capabilities (technological infrastructure, resources, awareness, and training) that underpin cybersecurity risk maturity. Market and technological turbulence are incorporated to reflect environmental dynamism and to test whether external conditions shape managerial risk perceptions and maturity outcomes.

1.4. Structure of work

The thesis is divided into six chapters. Chapter 1 articulates the research problem, states the research questions and objectives, develops the hypotheses, and outlines the sources, methods, and structure of the dissertation. It also situates the study in the context of accelerating digitalization and increasing cyber threats.

The second chapter presents the definition of cybersecurity, technical and market turbulence, cybersecurity governance, and the effects of cybersecurity investment. The third chapter highlights cyber-resilience as the core of business continuity. According to the Business Continuity Institute (2024), cyber resilience is central to operations and business continuity. First, a management process that identifies potential risks to an organization and provides a framework for resilience will be defined to clarify the determinants of business continuity. It

will then elaborate on the need for Business Continuity Planning (BCP) and the details of aspects of business cyber resilience. The role of context and the importance of cyber resilience to companies' activities will be provided, followed by a list of global assessments of organizational resilience (e.g., ISO 22301; NIST CSF 2.0).

The fourth chapter deals with the role of cybersecurity risk maturity in shaping resilience. It comprises four parts covering the key components of risk maturity, a global overview of maturity assessments, the impacts of maturity on resilience, and its measurement. In this regard, previous research will likewise be provided by assessing cybersecurity risk maturity. In this context, the fifth chapter empirically examines the association between organizational resilience and the maturity of cybersecurity risk management. It includes a brief sketch of the study's limitations, an explanation of the research methodology, results analysis of the findings, and recommendations for further research. Data is collected using a survey questionnaire. Chapter 6 (conclusion) synthesizes the thesis and provides an overview of the main findings, limitations, and suggestions for future work. The expected impact of the present study on cybersecurity risk maturity is evident in its innovative multidimensional approach to assessing an organization's cyber resilience. Previous research confirms that, for cyber resilience to be achieved, a proactive, risk-based approach must be adopted: actively conduct effective risk assessments and implement continuous, proactive measures to protect the organization. Conklin et al. (2017) argued that a cyber-resilient strategy, focused on the selective and unconditional protection of critical assets, can enhance an organization's ability to withstand and recover from cyberattacks. Such an extensive investigation enables us to identify critical determinants of cybersecurity risk maturity, including the evolution of security measures, the alignment of the IT approach with organizational security objectives, and the development of a cybersecurity-oriented organizational culture supported by leadership. Previous studies have assessed diverse determinants individually, but comparative analyses have not integrated these factors as antecedents of resilience improvement. Furthermore, the literature examining the effects of cybersecurity risk maturity across organizational contexts is scarce. By examining factors such as cybersecurity risk maturity and resilience, this thesis seeks to provide organizations with actionable insights to strengthen their cybersecurity frameworks.

1.5. Scientific contribution

This dissertation examines the determinants of cybersecurity risk maturity and their impact on organizational resilience. The **first** contribution is a specification and validation of a combined

capability–governance model that ties cybersecurity risk maturity to organizational resilience. Building on conceptualizations of cyber resilience, this research operationalizes cybersecurity risk maturity as an institutionalized lifecycle of risk identification, assessment, mitigation, and continual improvement. As such, it reveals that maturity serves as a primary proximal mechanism for achieving resilience in organizations and reframes resilience from a passively observed phenomenon to something deeply rooted in routinized, governance-assisted risk-management practices.

The **second** contribution is the empirical validation of a multi-layered antecedent structure of cybersecurity risk maturity, encompassing a complex set of factors that coalesce to produce it, including technological, organizational, human, relational, and governance drivers. Most previous work treats these domains in parallel rather than as co-observed effects within a single structural system: infrastructure safety, resource availability, process formalization, and human factors in security behavior. The study describes that technological infrastructure and cybersecurity resources/capabilities serve as the base enablers of maturity. At the same time, alliance and collaboration mechanisms, risk perception, and support from top management are upstream enablers that shape these internal capabilities. It gives a more complete picture of the combined effect of internal and external factors on mature, resilience-supportive cybersecurity risk management.

The **third** contribution is the incorporation of environmental and construct-level refinements into the cyber resilience framework. The research, also highlighting market and technological turbulence as context, illustrates how environmental dynamism affects top management's risk perception and support, and, indirectly, collaboration and capabilities, without explicitly undermining maturity. Furthermore, the thesis shows empirical overlap between conceptually associated domains, especially awareness and training, and the governance connection between risk perception and support. This motivates further theoretical exploration, including consideration of higher-level constructs such as human capability and governance, and opens avenues for future research into the boundary conditions under which the domain operates as an independent or integrated feature of cyber resilience capability architectures.

2. THE NOTION OF CYBERSECURITY

This chapter provides a detailed assessment of the cybersecurity landscape and the dissertation's core constructs. It starts with a formal definition of cybersecurity. It details state-of-the-art models and standards that underpin organizational security practices, including those from NIST and ISO. The chapter then systematically operationalizes the primary constructs of the research model: cybersecurity risk maturity, technological infrastructure, cybersecurity resources and capabilities, cybersecurity awareness and training, cybersecurity alliances and collaborations, top management risk perception and support, and market and technological turbulence factors. Each construct is grounded in theory and positioned within the broader context of digital transformation and organizational strategy.

2.1. Definition of cybersecurity

The growing dependence on digital systems, including cloud computing, has made cybersecurity a critical global concern (Rajan et al., 2021; Subashini & Kavitha, 2011). Cybersecurity fundamentally involves protecting digital assets, individuals, and the overall cyber environment from cyber threats through strategies and technologies that prevent unauthorized access, destruction, or alteration of data (Cherdantseva & Hilton, 2013). Mukhopadhyay et al. (2019) developed a quantitative framework for cyber risk assessment, while Rothrock et al. (2018) emphasized that cybersecurity is a strategic business risk requiring board-level attention. Given these situations, global cooperation is essential. Therefore, organizations and national security entities are working together extensively through structured information-sharing frameworks, such as standardized threat intelligence protocols, to gain early insight into large-scale cyber threats (Fransen et al., 2015).

The cybersecurity environment is continuously evolving, driven by technological advances (Rajan et al., 2021) and the advanced tactics employed by malicious cyber adversaries (Kaur & Ramkumar, 2022; Rajasekharaiah et al., 2020). Previous studies have focused on developing a robust cybersecurity foundation, reviewing emerging encryption techniques, including quantum cryptography (Kaur & Ramkumar, 2022), and examining comprehensive cybersecurity policy frameworks (Azmi et al., 2018). In addition, human-centered cyber defense is highlighted, including the effects of cybersecurity policy awareness on employee compliance behavior (Li et al., 2019) and the influence of human factors on the definition and management of cybersecurity risk (Cains et al., 2022). To address the ongoing nature of cyber

threats, multiple areas of expertise in computer science, psychology, and law must collaborate to develop an integrated protection and resilience strategy grounded in risk assessment (Cebula et al., 2014; Cains et al., 2022). To sustain cybersecurity, it is essential to consider risk maturity and its impact on organizational resilience. Cyberattacks threaten critical infrastructure, jeopardizing public safety and the economy. This necessitates a comprehensive response encompassing technology, policy, education, and international cooperation (Cebula et al., 2014; CISA, 2023a; Cains et al., 2022).

Conceptual foundations

In recent years, the prevailing understanding of cybersecurity has departed sharply from traditional views of information security, mirroring the increasing complexity and interactivity of the digital landscape in the 21st century (Panteli et al., 2025; Azmi et al., 2018; Cains et al., 2022). In the age of accelerated digitalization across all areas of society, the conceptual boundaries of cybersecurity have expanded beyond a mere technical protection system to encompass a governance structure that addresses socio-technical issues, stakeholder responsibilities, and systemic risks (Panteli et al., 2025; Burch et al., 2024; Spremić & Šimunic, 2018). This requires addressing security within human, societal, and organizational dimensions (Panteli et al., 2025; Cains et al., 2022; Durst et al., 2024).

Modern academic literature recognizes cybersecurity as an intricate, multi-dimensional model encompassing techno-centric, human-centric, organization-centric, and societal dimensions, while also illustrating collective perspectives that set boundaries for responsible cybersecurity practice (Panteli et al., 2025). This multilevel frame of reference arises from empirical research with senior cybersecurity professionals, who emphasize that successful cybersecurity is a multifaceted, holistic process that requires commitment from multiple stakeholders, who steward not only their own data but also supply chain partners and the greater good (Panteli et al., 2025).

Tan et al. (2025) examine the relationship between cybersecurity governance and corporate market value from the perspectives of investor trust and supply chain trust. More broadly, the systematic perspective on responsible cybersecurity draws on the multi-layered framework of Panteli et al. (2025), which emphasizes stakeholder responsibilities across techno-centric, human-centric, and societal dimensions. The definition of cybersecurity is becoming increasingly complex due to the constantly evolving threat landscape, technological

capabilities, and regulatory requirements of the digital age (Cains et al., 2022; Azmi et al., 2018).

Recent systematic literature reviews have identified numerous definitions of cybersecurity in academic and practitioner literature, indicating broad disagreement over which dimensions accurately define the scope, objectives, and techniques for achieving cybersecurity outcomes (Büyüközkan & Güler, 2025; Brezavšček & Baggia, 2025). Far from being merely an academic issue, this proliferation of definitional terms is manifested in policy dilemmas, organizational strategies, and international action against transnational cyber threats (Fahey, 2024; Azmi et al., 2018). Applying the resource-based view, the extant cybersecurity academic literature situates cybersecurity capabilities as strategic organizational resources that provide a sustained competitive advantage when they are valuable, rare, inimitable, and organizationally embedded (Durst et al., 2024; Järveläinen et al., 2025). This theoretical model suggests that cybersecurity success relies not only on investments in technology but also on organizational capabilities, human competencies, and governance systems that facilitate adaptive responses to dynamic threat environments (Durst et al., 2024; Panteli et al., 2025). Cybersecurity has also been shown to constitute a valuable organizational capability for companies that apply established governance processes. Mature cybersecurity risk management practices are positively associated with organizational resilience (Durst et al., 2024). In contrast, strong cybersecurity governance can boost corporate market value through mechanisms of reputation building and investor trust (Tan et al., 2025).

The integration of artificial intelligence and machine learning with cybersecurity has significantly redefined definitional boundaries and operational paradigms, creating opportunities for automated threat detection and new forms of vulnerabilities and ethical concerns (Dal Cin et al., 2025; NIST, 2024). Recent academic research acknowledges the integral position of machine learning in fighting cyberattacks (Razzaq & Shah, 2025). Nevertheless, the implementation of artificial intelligence technologies also raises key issues regarding algorithmic bias, transparency, and accountability in cybersecurity decision-making (Barredo Arrieta et al., 2020).

Historical evolution and contemporary developments

The evolution of cybersecurity definitions mirrors broader trends in the adoption of digital technology, the sophistication of attacks, and regulatory responses (Azmi et al., 2018; Cains et al., 2022). In contrast to earlier periods, when the emphasis was primarily on perimeter defenses

and technical controls, cybersecurity now entails an integrated risk management approach that addresses supply chain vulnerabilities, third-party dependence, and systemic risks spanning organizational boundaries (Panteli et al., 2025; NIST, 2024). This evolution reflects the growing recognition that cyberattacks are increasingly occurring at scale by exploiting interconnections and dependencies within complex networks and digital ecosystems, rather than targeting isolated systems or organizations (Porambage & Liyanage, 2023). The 2020 to 2025 period has been especially transformative for cybersecurity conceptualization, driven by the accelerated digital transformation during the COVID-19 pandemic and the concurrent expansion of attack surfaces in remote work technologies, cloud-based computing, and digital health systems (Dal Cin et al., 2025). The evolution toward these more advanced and responsive cybersecurity paradigms is exemplified by the adoption of zero-trust security architectures and identity-centric security models (NIST, 2020; NIST, 2024).

The rapid growth of research at the intersection of machine learning and cybersecurity underscores the need to integrate advanced technologies into modern cybersecurity strategies and practices (Razzaq & Shah, 2025). Forward-looking views like these recognize that cybersecurity is not a static field but rather evolves in response to technological advancements and shifting threat landscapes (Brezavšček & Baggia, 2025; Järveläinen et al., 2025). More recently, the growing sophistication of nation-state cyber activities and the persistence of threats have broadened the definition of cybersecurity to encompass geopolitical domains, international law, and diplomatic actions in the context of cyber incidents (Fahey, 2024). Recent research suggests that cybersecurity cannot be perceived solely as a technical or organizational problem; it also requires consideration of the broader political, economic, and social factors that may shape assessments of threat actors' motivations and capabilities (Panteli et al., 2025). This broader perspective recognizes that, at its essence, cybersecurity is a socio-technical phenomenon that requires interdisciplinary work and multi-stakeholder coordination (Panteli et al., 2025).

Key components and contemporary frameworks

The ever-evolving nature of digital security challenges calls for continuous adaptation of conceptual frameworks, practical approaches, and governance mechanisms (Brezavšček & Baggia, 2025); hence, the ongoing debate over a definition of cybersecurity. In order to bridge this gap, future research and practice should develop more flexible, inclusive, and actionable definitions of what constitutes cybersecurity that can accommodate technological innovation,

the emergence of new threats, and the needs of organizations and society, while also providing a guide for decision-making and implementation (Panteli et al., 2025). These frameworks play an integral role in the creation of knowledge and practice of cybersecurity in our digitized and connected world (Panteli et al., 2025).

Modern cybersecurity frameworks identify five key elements that collectively provide frameworks for the implementation of reliable cybersecurity techniques and principles: techno-centric elements, or technological defenses; human-centric components, or user experience and workforce; organizational factors, which address internal governance systems and cultures; inter-organizational dimensions, or supply chain and partnership security; and societal considerations, which are a recognition of the broader social scope of cybersecurity decisions (Panteli et al., 2025). This multifaceted framework (Table 1) transcends traditional technical paradigms and is grounded in empirical insights from senior cybersecurity professionals (Panteli et al., 2025).

Table 1: Five core components of modern cybersecurity frameworks

Component	Key Elements	Primary Focus
Techno-Centric Components	Artificial intelligence, machine learning, Behavioral analytics, Automated response systems, Zero-Trust architecture, Identity-centric security, Cloud security, Edge computing	Technological defenses
Human-Centric Components	User behavior and decision-making, Workforce wellbeing, Behavioral change initiatives	Individual well-being and user-centric design
Organizational Components	Governance mechanisms, Risk management systems, Incident response capabilities, Organizational culture, Training and	Shared responsibility and organizational culture

	awareness programs, Cultural factors, Leadership commitment, Resource allocation	
Inter-Organizational Components	Supply chain security, Partnership security, Third-party risk management, Vendor assessment, Collaborative threat sharing	Supply chain and external impact
Societal Considerations	Geopolitical aspects, International law and diplomatic responses, Regulatory frameworks, Socio-technical perspectives	Wider societal impacts

Source: Author's work (based on Panteli et al., 2025)

Techno-centric components

The techno-centric approach to modern cybersecurity employs state-of-the-art technologies, including artificial intelligence, machine learning, behavioral analytics, and automated response systems, to help organizations detect, analyze, and respond to cyber threats at scale (Dal Cin et al., 2025; Lee, 2023). Recent scientometric studies of the cybersecurity literature indicate that machine learning techniques, including supervised and unsupervised classification methods, are among the fastest-growing research areas (Razzaq & Shah, 2025). Artificial intelligence enables cybersecurity operations to implement innovations such as threat hunting, anomaly detection, and predictive risk assessment, while also introducing new challenges, including algorithmic bias, adversarial attacks, and explainability requirements (Razzaq & Shah, 2025). The effectiveness of these technologies depends heavily on user adoption, usability, and integration with organizational processes, underscoring the need for human-centric design (Panteli et al., 2025). This view stands in stark contrast to earlier paradigms that prioritized technical competency over user experience and organizational fit (Panteli et al., 2025).

Technologies with poor usability often fail to deliver intended security benefits due to user workarounds and noncompliance (Panteli et al., 2025). Contemporary architecture must support dynamic, heterogeneous technology ecosystems and enforce consistent security policies across platforms (NIST, 2020). This architectural development represents the transition from perimeter-based to zero-trust security models, which require no implicit trust based solely on network location (NIST, 2020; CISA, 2023b).

Human-centric components

The human-centric approach emphasizes that successful cybersecurity relies heavily on human behaviors, decisions, and organizational culture, rather than solely on technical controls (Panteli et al., 2025). A user-centered approach is vital for designing solutions that protect workers from stress and burnout, reflecting the recognition that cybersecurity is a human endeavor shaped by psychological, social, and cultural factors (Panteli et al., 2025).

Recent developments in cybersecurity education and awareness activities extend beyond conventional compliance-centered training by emphasizing adaptive, role-sensitive, and continuously improved programmes (He & Zhang, 2019; Hatzivasilis et al., 2020; Chowdhury et al., 2022). Effective cybersecurity education benefits from iterative reinforcement, tailored content, and alignment with organizational needs rather than relying only on generic, one-time awareness materials (He & Zhang, 2019; Hatzivasilis et al., 2020; Chowdhury et al., 2022). The international shortage of qualified cybersecurity professionals poses challenges for organizations seeking to build robust defense capabilities, a challenge exacerbated by a significant global shortage of cybersecurity professionals ((ISC)², 2023). Emerging research highlights the need for integrated workforce development approaches that incorporate multiple pathways into the cybersecurity workforce, career development, continuing education, and retention strategies ((ISC)², 2023). Building cybersecurity workforce skill sets will be a joint venture among educational institutions, employers, professional organizations, and government agencies to design sustainable talent pipelines and career pathways ((ISC)², 2023).

The organizational components

Organizational components include governance mechanisms, risk management systems, incident response capabilities, and cultural factors that address cyber risks and reinforce business objectives. Recent literature argues that cybersecurity governance requires aligning the interests of organizational principals and agents, supported by appropriate incentive

structures and monitoring mechanisms to manage cyber risks effectively (Burch et al., 2024). The relevance of agency theory to cybersecurity governance is also evident in the need for appropriate incentive frameworks, monitoring, and performance mechanisms that link cybersecurity efforts to organizational goals (Burch et al., 2024). Current cybersecurity risk management paradigms have shifted from compliance-oriented controls to holistic enterprise risk management mechanisms that link cybersecurity risk to other business and strategic risks (Burch et al., 2024).

The emergence of cybercrime demands that organizations' security and information technology systems be integrated and maintained strategically. Empirical studies show that organizations with more mature cybersecurity risk management capabilities demonstrate greater organizational resilience (Durst et al., 2024). The organizational cybersecurity culture has since become one of the most vital determinants of cybersecurity effectiveness (Panteli et al., 2025). Modern approaches to building, nurturing, and sustaining cybersecurity cultures focus on leadership modeling, the understanding and communication of expectations, recognition and reward systems, and the weaving of cybersecurity values into broader organizational culture programs (Burch et al., 2024; Panteli et al., 2025).

Significance in modern organizations

The centrality of cybersecurity stems from its role in protecting digital operations and sustaining competitive advantage. The widespread adoption of cloud computing, the Internet of Things, and remote work—accelerated by the COVID-19 pandemic—has expanded the attack surface and created complex interdependencies (Porambage & Liyanage, 2023; Dal Cin et al., 2025). Consequently, strong cybersecurity governance is no longer merely a compliance concern but a strategic business enabler that increases a firm's market value, reputation, and investor trust (Tan et al., 2025). Given the sophistication of ransomware and supply chain attacks, cybersecurity is a board-level imperative necessitating strategic planning and resource allocation. Cyber incidents can severely diminish brand value and stakeholder relations long after technical recovery, making comprehensive cybersecurity programs essential for regulatory compliance and market competitiveness (Tan et al., 2025).

Legal and regulatory context

Since 2015, the regulatory environment in cybersecurity has been transformed by the gradual scaling up of new directives, enforcement measures, and international collaboration, evidencing

the recognition and prioritization of cybersecurity in international policy (Fahey, 2024). Modern regulatory frameworks emphasize risk-driven approaches, mandatory incident reporting, and sector-specific standards that account for distinct security risks and capabilities across sectors and enterprise types (European Parliament and Council of the European Union, 2022a; Securities and Exchange Commission, 2023). The evolution of global cybersecurity norms and cooperation structures highlights the transnational nature of cybersecurity threats and the need for joint action beyond national borders (European Union Agency for Network and Information Security, 2018).

Recent regulatory actions include mandatory cybersecurity information reporting by publicly traded corporations, protection of critical infrastructure, and data protection laws that impose significant compliance obligations and create potential liability for entities with inadequate cyber hygiene (Securities and Exchange Commission, 2023; European Parliament and Council of the European Union, 2022a). The EU's NIS2 Directive, which entered into force in 2023, imposes substantial cybersecurity requirements on a wide range of businesses and harmonizes cybersecurity across EU member states (European Commission, 2023). Similar regulations, now introduced in other jurisdictions, reflect a global trend toward increasingly comprehensive and enforceable cybersecurity requirements (Swiss Financial Market Supervisory Authority (FINMA), 2022; Securities and Exchange Commission, 2023). The convergence of cybersecurity regulation with data protection, privacy, and artificial intelligence governance presents a nuanced set of compliance hurdles. It will require a composite approach to legal and regulatory risk management (Fahey, 2024; European Union, 2024). Modern companies are confronted with several overlapping (and sometimes competing) regulatory pressures that should be balanced to achieve operational efficiency on the one hand and innovation on the other (Fahey, 2024).

Emerging trends and future directions

Contemporary cybersecurity research identifies several important trends that will substantially influence security definitions, practices, and governing paradigms (NIST, 2024). Quantum computing capabilities will necessitate a new era for cryptographic techniques, security frameworks, and threat models (NIST, 2024).

Studies emphasize ethical measures and explainable artificial intelligence to ensure human trust and control in artificial intelligence-driven security decisions (Razzaq & Shah, 2025). This will address the issue by exploring the development of explainable artificial intelligence capabilities

for cybersecurity applications to meet human understanding and trust needs in artificial intelligence-driven security decision-making (Razzaq & Shah, 2025). Furthermore, cybersecurity has evolved into an ecosystem-based paradigm that leverages collective defense and information sharing to address complex threats, thereby strengthening overall cyber resilience (European Union Agency for Network and Information Security, 2018). The emergence of public-private partnerships, industry consortia, and international cooperation mechanisms represents a fundamental shift toward more integrated and collaborative forms of cybersecurity governance (European Union Agency for Network and Information Security, 2018).

Challenges in defining cybersecurity

Defining cybersecurity involves navigating persistent tensions between theoretical accuracy and practical utility, organizational autonomy and collective security, and innovation and risk management (Panteli et al., 2025). Recent academic research indicates that numerous definitions of cybersecurity exist in the scholarly and practitioner literature (Brezavšček & Baggia, 2025; Panteli et al., 2025), underscoring the continued lack of consensus on fundamental concepts, scope, and objectives. This definitional expansion creates operational challenges and policy and regulatory concerns, necessitating attention to organizational planning and global collaboration (Panteli et al., 2025). Keeping abreast of the evolving definition of cybersecurity amid rapid technological change is a significant challenge (Brezavšček & Baggia, 2025).

Modern definitions of cybersecurity must be as applicable and adaptable as possible to the changes in new technologies, evolving threats, and the organizational environment (Panteli et al., 2025). Given the interdisciplinary nature of cybersecurity, contemporary cybersecurity definitions must serve professionals across various domains (technical specialists, managers, policymakers, and academic researchers) and be helpful and reusable across different career segments (Panteli et al., 2025). Stakeholder communities hold different perspectives on cybersecurity and employ distinct vocabularies and priorities (Panteli et al., 2025). As a result, communication and alignment between these communities may become confused or misaligned, thereby impeding cooperation (Panteli et al., 2025). Developing shared terminology across professional communities can improve cybersecurity communication and coordination (Cains et al., 2022; Fischer-Hübner et al., 2021).

2.2. *Cybersecurity risk maturity*

Cybersecurity Risk Maturity (CSRM) is an advanced, comprehensive, and systematic approach to identifying, assessing, managing, and continuously improving cybersecurity risk management capabilities across all levels and functions of the enterprise. Defining cybersecurity risk maturity serves several functions: helping organizations assess their capabilities, work toward improvement, and develop strategic roadmaps to enhance their cybersecurity posture (Durst et al., 2024; Brezavšček & Baggia, 2025). The Swiss approach reflects that mature organizations must change from reactive measures to proactive, governance-led approaches, guided by documented approaches based on the NCSC ICT Minimum Standard (Federal Office for National Economic Supply, 2023), also in light of the aim of NCS to reduce cyber risks systematically (Federal Council, 2023; FINMA, 2022). According to the latest research, cybersecurity risk maturity entails integrating multiple frameworks and standards, such as EU NIS2 Directive-level requirements for organizations engaged in EU activities (European Commission, 2023) and, where applicable, the Digital Operational Resilience Act (DORA) for financial entities (European Parliament and Council of the European Union, 2022a). Recent systematic literature reviews have identified significant shortcomings in existing maturity models, including a lack of real-world testing and validation (Proença & Borbinha, 2016; Rabii et al., 2020; Poeppelbuss & Röglinger, 2011) and the absence of tailored models for specific organizational types (Ahmad et al., 2024).

Risk identification and assessment methodologies

Mature cybersecurity requires systematic, organization-wide methodologies for identifying and classifying risks across all business areas and third-party providers. The Swiss approach insists that the risk identification methodology must include enterprise-wide business operations and critical third-party providers, aligned with the NIST Cybersecurity Framework 2.0 Govern and Identify functions (NIST, 2024), ISO/IEC 27005:2022 risk management guidance (ISO, 2022a), and COSO enterprise risk management principles (COSO, 2017), with assessment conducted at least annually and following significant changes in the organization's risk profile, threat environment, or regulatory requirements (Federal Council, 2023; FINMA, 2022). Artificial intelligence and machine learning technologies, which can identify previously undocumented patterns and associations, have enhanced the scope and sophistication of risk identification (Kure et al., 2022; Dal Cin et al., 2025; Pejić Bach et al., 2023).

Threat intelligence integration and risk assessment

Formalizing external threat intelligence within risk assessment processes is a key element of cyber risk maturity. Leading frameworks require a systematic outline for incorporating external threat intelligence into risk assessment procedures, including documented processes and impact analyses for relevant threats (NIST, 2024; Kure et al., 2022). Robust threat-intelligence integration, therefore, hinges on organizations developing sophisticated capabilities to collect, analyze, and act on threat intelligence from diverse streams, including commercial threat intelligence feeds, government sources, and industrial threat-sharing initiatives. Organizations can better adapt their security posture to emerging threats by prioritizing threat intelligence over reactive measures based on threat status.

Comprehensive risk register management

An organization must maintain a comprehensive risk register with regular updates, reviews, and validation processes, and store those risks centrally in a data repository. Leading frameworks state that consolidated risk inventories for all identified problems should be stored in central repositories, regularly maintained, and periodically reviewed to ensure they comprehensively cover all critical areas of the business (NIST, 2024; COSO, 2017). Contemporary risk register management approaches focus on a dynamic risk assessment capability that accounts for the rapidly changing threat and business environments.

Governance integration and board-level oversight

A formal convergence between cybersecurity risk management and organizational governance, including regular board reporting, is a significant aspect of risk maturity. This aligns with the NIST CSF 2.0 Govern function (NIST, 2024) and DORA Article 5 on ICT risk management governance (European Parliament and Council of the European Union, 2022a). Good governance integration requires sophisticated reporting capabilities that translate technical risk assessments into business-impact assessments relevant to senior leadership and the board. This ensures the proper integration of cybersecurity components into strategic planning processes and supports decision-making regarding cybersecurity investments and risk tolerance.

Framework adoption and implementation

Adoption and implementation of comprehensive cybersecurity frameworks constitute a primary measure of risk maturity, and organizations must demonstrate compliance with and full implementation of the framework across a range of functions and business contexts. Framework

based assessment requires evidence of the formal adoption and progressive implementation of holistic cybersecurity frameworks and models (for example, NIST CSF 2.0, Zero Trust Architecture), maturity assessments, and continuous improvement processes designed based on organizational risk profiles (NIST, 2024; NIST, 2020; ISO, 2022a; CISA, 2023b; CISA, 2020). Companies must ensure that frameworks are compatible with existing infrastructure and employ change management practices to yield meaningful improvements in risk management. This capacity allows organizations to be assured that implementing frameworks yields meaningful improvements in risk management, without arbitrarily imposing requirements from outside the organization.

Risk mitigation and control effectiveness

Organizational data-driven documentation can demonstrate that the security control measures they implement effectively mitigate identified risks (NIST, 2024; ISO, 2022a). Issue information documents at regular intervals to align with the NIST CSF 2.0 Protect function. Risk accounting methodologies, such as FAIR, can provide a structured process for measuring financial terms of effective control (Jones, 2006; Freund & Jones, 2014). Modern cybersecurity risk management selects, implements, and evaluates security controls according to identified risks, organizational context, and risk-treatment priorities (ISO, 2022a; NIST, 2024). Organizations should also conduct cost-benefit analyses and document the benefits of primary risk mitigations, using defined risk-quantification methodologies to justify ROI (Freund & Jones, 2014; ISACA, 2022).

Continuous monitoring and risk assessment

A continuous monitoring approach to security controls and risk levels is critical to cybersecurity risk maturity, and firms seeking to adopt it must implement automated tools and systems that provide near-real-time visibility into their risk posture in the early stages. Under both international and Swiss supervisory expectations, the effectiveness of security control measures and risk-level monitoring should be assessed on an ongoing or near-continuous basis using automation tools or systems, with mechanisms in place to guide the management of critical control failures (NIST, 2024; FINMA, 2022). For continuous monitoring, organizations must develop sophisticated data-collection and analysis capabilities to process large volumes of security data and identify key patterns and trends. Continuous monitoring requires advanced analytical capabilities that can process large volumes of operational and security-relevant data, utilizing predictive modeling, automated detection techniques, and advanced data analytics,

including text mining, to identify anomalies, emerging patterns, and hidden risk indicators, particularly within complex environments, such as large financial datasets (Pejić Bach et al., 2019; NIST, 2024). Ultimately, these capabilities enable a transition from merely reacting to security incidents to proactively managing risk.

Executive reporting and risk communication

Effective executive reporting and risk communication must translate technical risk assessments into business impact assessments that prompt senior leadership to act. Business requires sophisticated reporting mechanisms, which mark its move beyond its simplest stage. The Swiss methodology mandates the ongoing tracking of recognized quantitative cybersecurity risk metrics, trend analysis, and their regular reporting to senior executive leadership (NIST, 2024). On a routine basis, the risk function needs to provide senior leadership with risk status and guidance on next steps, including risk dashboards and trend analyses (NIST, 2024; Burch et al., 2024). Regulatory frameworks increasingly mandate that management bodies report on ICT risk (European Parliament and Council of the European Union, 2022a). This functionality enables sound decision-making regarding investments and risk-management targets.

Assessing risk maturity and continuous improvement

When organizations assess the maturity of their cybersecurity risk management, they need to implement systematic evaluation processes to measure progress. It calls for the development of sophisticated assessment methodologies that analyze multiple dimensions of risk management capability, enabling organizations to assess their ability to deliver on their promises. Continuous improvement in this age of maturity requires systematic risk and capability management to identify, assess, and implement design improvements. This means that risk management must continually evolve to keep pace with new threat landscapes (and business trends) and ensure business objectives are met. Organizations must continue to address these issues to maintain effective risk management across their operations.

2.3. Cybersecurity resources

2.3.1. Technological infrastructure

Technological Infrastructure (TI) comprises hardware, software, networking, cloud services, and electronic platforms interconnected to support organizational performance, data integrity, and cybersecurity (Aldea et al., 2023; Nadji, 2024; Shahim, 2021). Within the Swiss context, technological infrastructure security needs to be aligned with the ICT Minimum Standard

recommendations (Federal Office for National Economic Supply, 2023), the National Cybersecurity Strategy provides the overarching strategic direction (Federal Council, 2023), and ICT infrastructure robustness needs for regulated financial institutions are detailed in the FINMA Circular 2023/1 (FINMA, 2022).

Infrastructure resilience and redundancy design

Technological robustness includes redundant processes, fault-tolerant processes, and the potential to scale by minimizing the risk of single points of failure (NIST, 2024). Higher maturity levels in cybersecurity risk models reflect institutionalized practices that enhance an organization's capacity to anticipate, withstand, and recover from cyber incidents (Brezavšček & Baggia, 2025; Rabii et al., 2020). At the same time, security measures, such as multi-layered defenses, encryption, and regular patch management, are fundamental in protecting information assets (NIST, 2024). This infrastructure should be preserved through structured governance and ongoing oversight, and adherence to cybersecurity standards (CISA, 2023a).

According to contemporary research, a robust technological infrastructure must integrate sophisticated security architectures with zero-trust principles, artificial intelligence, and resilient design patterns that evolve with time while maintaining operational effectiveness. The evolution of cybersecurity technologies is driven by the realization that conventional perimeter security models are insufficient in contemporary threat environments, necessitating resilient and redundant infrastructure designs. Critical systems must maintain redundancy configurations with automatic failover capabilities and uptime levels determined by Business Impact Analysis (ISO, 2019; Business Continuity Institute, 2024), and disaster recovery infrastructure must be regularly tested to validate recovery objectives. To achieve high uptime, risk-factor redundancy schemes must meet those parameters. This allows organizations to withstand even severe disruptions, such as hardware component failures or major power failures, without disrupting normal infrastructure operations.

Security architecture and secure-by-design principles

Organizations need to build resilient infrastructure to maintain control in the event of failure, avoid a complete system breakdown, and enable automatic failover. This redundancy is essential when system availability directly impacts business operations and customer service delivery, necessitating adherence to secure-by-design principles and component best practices. Modern security architecture frameworks focus on security controls embedded in the IT

environment throughout their lifecycle, and on adopting secure-by-design approaches to technology development (NIST, 2024). This has been shown in domains such as cyber-physical systems engineering, where security requirements are traced from system-level design to implementation (Geismann et al., 2018). The goal is to integrate security seamlessly into technology's physical fabric and operational processes, rather than superimposing it as an afterthought.

The use of advanced cybersecurity technologies is a key component of an organization's IT infrastructure (Malatji et al., 2022). These technologies enable dynamic risk mitigation, allowing real-time threat detection and the development of adaptive defense mechanisms (Prakash et al., 2024). The compatibility between deploying cutting-edge technology and promoting organizational resilience is supported by resilience theory, which asserts that resilient systems can predict, absorb, and recover from cyber disruptions (Malatji et al., 2022). Empirical evidence indicates that organizations with high cybersecurity maturity systematically adopt advanced technical tools to enhance situational awareness (Dal Cin et al., 2025). Enterprises require sophisticated design and development practices that account for security implications at every stage of the technology lifecycle to instill secure-by-design principles. This capability helps users detect and address security issues before deploying them to production environments.

Stress testing and performance validation

Organizations must document and review verification of their infrastructure's operational and security status during attack drills, demand peaks, and stress-testing periods (NIST, 2024; CISA, 2023a). Testing must realistically simulate threat scenarios and operational conditions to make meaningful assessments of infrastructure resilience. Rolling out effective test capabilities is complex, so organizations need to adopt advanced techniques that model complex attack scenarios and evaluate performance on infrastructure under a range of stress conditions. This enables organizations to identify and remediate vulnerabilities before they are exploited.

System integration and interoperability

Technology platforms and security tools must ensure data sharing in accordance with documented integration frameworks, support centralized logging, and enable monitoring to create a full enterprise view (NIST, 2024; Aldea et al., 2023). This integration enables a more complete security posture and better response to threats that traverse multiple systems or

platforms. Successful system and data integration depends on a range of complex techniques that work across different technology platforms and data formats. This process is particularly crucial in a highly centralized environment where legacy applications must be integrated into modern cloud-based platforms, applications, and services used by other organizations.

The scalability design and cloud-native principles

A scalable technology infrastructure that adapts to business needs while maintaining security requires implementing cloud-native principles and conducting documented scalability assessments (NIST, 2024; Lee, 2023). This ability helps enterprises maintain adequate security measures as they expand and evolve their operations. To implement scalable infrastructure, organizations should develop advanced capacity planning and management capabilities to anticipate future requirements and ensure that security scales with the business. Such capability is especially relevant for rapidly growing organizations or for situations in which operating requirements or circumstances are changing rapidly.

Unified security management and centralized control

Unified security management integrates security capabilities to ensure comprehensive protection across diverse technology environments through centralized tracking, oversight, and policy enforcement (NIST, 2024; Nadji, 2024). This integration is powerful because it enables companies to develop unified security policies and practices across all technology platforms and environments. Unified security management can be achieved only by organizations that implement sophisticated security orchestration and management platforms that integrate diverse security tools and technologies into cohesive management frameworks. This ability empowers security teams to gain comprehensive visibility into the organization's security posture, thereby enhancing threat detection and response.

Advanced cybersecurity technology development

Organizations need modern security technologies, including artificial intelligence-driven threat detection, zero-trust architecture, advanced analytics, and more, to implement these capabilities across infrastructure, with documented effectiveness metrics and regular capability reviews (NIST, 2024; NIST, 2020; CISA, 2023b; Yan et al., 2023). To assess high-tier threat detection, an organization must also use known metrics such as mean time to detect (MTTD), detection accuracy, and response time (NIST, 2024; CISA, 2023a), aligning with industry benchmarks

and risk tolerance. The company needs advanced capabilities to evaluate and integrate cybersecurity technologies.

Threat detection and response capabilities

Advanced threat detection requires robust monitoring, detailed performance metrics, and mechanisms to capture and characterize diverse threat behaviors (Sarker, 2021). These features require continuous evaluation and improvement to stay relevant in changing threat environments. Effective threat detection capabilities can only be built within organizations that construct and communicate high-quality data systems capable of handling large volumes of data, where attackers can leverage security-related information to extract significant patterns and anomalies. This can enable organizations to identify threats earlier and respond more quickly, thereby reducing the magnitude of security incidents.

Technology evolution and innovation adoption

Organizations must document evaluation criteria and implementation procedures for innovative technologies to ensure systematic and risk-informed adoption (NIST, 2024; Prakash et al., 2024). This enables organizations to leverage new technologies to enhance defenses while balancing emerging risks. Adoption requires a rigorous risk-benefit analysis to determine organizational fit and feasibility. This capability provides a competitive advantage by facilitating the strategic adoption of useful technologies while preventing premature or improper implementation.

2.3.2. Cybersecurity resources and capabilities

Cybersecurity Resources and Capabilities (CSRC) comprise human capital, technological resources, financial investments, and organizational processes that support the efficient and effective management of the organization, ensuring resilience and responsiveness to cyber threats. The Swiss National Cybersecurity Strategy explicitly highlights the need for greater resources and capabilities (Federal Council, 2023), a requirement that is indirectly addressed in the ICT Minimum Standard (Federal Office for National Economic Supply, 2023) but applied directly to critical entities by the EU NIS2 Directive (European Commission, 2023). Modern literature notes that successful resource management must be informed by alignment between risk and organizational goals, as well as by the equilibrium between resource allocation and operations to maximize security efficacy (Burch et al., 2024; Gordon & Loeb, 2002). The CISA Cross-Sector Cybersecurity Performance Goals provide baseline security measures for critical

infrastructure organizations (CISA, 2023a). Research recognizes that success in cybersecurity transcends technical capabilities; the human factor must co-exist with organizational factors to achieve effective security outcomes (Panteli et al., 2025; Glaspie & Karwowski, 2018).

Human capital development and talent management

The development and management of qualified cybersecurity talent are among the most important pillars of an organization's cybersecurity capabilities, and organizations must implement specific talent management strategies to support recruitment, retention, professional development, and succession planning. Retention and succession planning should be used to maintain security teams, supported by structured human resource metrics, to keep the workforce aligned with the organization's threat profile (ISACA, 2022; (ISC)², 2023). In the Swiss context, the National Cybersecurity Strategy highlights the importance of adequate cybersecurity capabilities (Federal Council, 2023). From cybersecurity to talent acquisition, cybersecurity skills shortages have become a major crisis for companies globally, forcing them to find innovative solutions to both attract and retain talent. In an increasingly competitive landscape, employers need a comprehensive program to develop internal capabilities and implement competitive compensation and career advancement strategies to attract and retain skilled workers.

Leadership qualifications and professional development

Cybersecurity leadership requires individuals with professional credentials (e.g., Certified Information Systems Security Professional, Certified Information Security Manager) and the "business acumen" necessary to translate technical requirements into strategic objectives and secure top-management support ((ISC)², 2023; ISACA, 2022). These programs must account for the specific challenges posed by cybersecurity leadership, including communicating with technical and business stakeholders, navigating complex risk trade-offs, and remaining relevant amid rapidly changing threat conditions.

Skills development and competency building

A formal professional development program, supported by appropriate training budgets and curricular planning, is essential for sustaining competence in cybersecurity within an organization, according to the NIST NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework (Paulsen et al., 2012). These services need to be customized to meet the organization's unique needs and aligned with identified competency

frameworks. Good skills development programs are supported by competency assessment systems that enable organizations to design targeted training programs to mitigate skills gaps; effective training programs must address these gaps through systematic measures. This capability enables organizations to maintain current and relevant cybersecurity skills as threat and technological landscapes evolve rapidly.

Advanced threat detection and organizational intelligence

Advanced threat detection and organizational intelligence Machine-learning-based threat-detection systems can be evaluated using detection-performance measures derived from observed data (Sarker, 2021; Muhati & Rawat, 2024). These systems should generate prioritized, low-noise alerts to ensure analyst efficiency and rapid response (Razzaq & Shah, 2025). As with solutions from other disciplines, these solutions require constant monitoring and fine-tuning to adapt to an ever-changing threat environment and attack vectors. Therefore, if organizations are to deploy next-generation threat detection technologies, a robust assessment and selection system must be adopted to evaluate them for use and select the most appropriate approaches for their specific environments and requirements. This capability enables organizations to leverage new technologies to enhance threat detection, thereby mitigating risks associated with investments in technologies that do not deliver tangible benefits.

Operational intelligence and alert management

Security tools should generate concise, prioritized alerts that elicit effective responses in accordance with documented alert management processes, with reasonable false-positive rates and response-time metrics (NIST, 2024; Razzaq & Shah, 2025). This feature necessitates a highly complex approach to adaptation and optimization that must align comprehensive threat detection with the practical constraints of alert volume and analyst efficiency. The development of operational intelligence capability is a task for organizations to support effective data analysis, a correlation system for detecting security events and information, and the filtering of noise and false positives. This feature enables security teams to focus on real threats rather than on managing low-priority alerts.

Technology lifecycle management

Technology lifecycle management requires systematic review and decommissioning of legacy tools to mitigate risks associated with unsupported technology and manage modernization costs (ISO, 2022b; NIST, 2024). These efforts enhance the effectiveness of security technologies by

continually innovating across the security life cycle. At the same time, these companies must manage the costs and complexity associated with technology modernization. To achieve this, effective lifecycle management of technology requires companies to establish a comprehensive framework for technology planning and budgeting that anticipates how often technology updates will be required at any given time or place. This feature protects organizations from the risks posed by outdated or unsupported technology and helps them manage modernization costs.

Risk-based financial management

Cybersecurity investment should be determined through risk-based analysis rather than a fixed percentage of the IT budget. The appropriate level depends on the expected loss, the vulnerability of the information set, and the effectiveness of security spending (Gordon et al., 2016). To create an effective budget allocation process, organizations must conduct advanced risk-based investment analysis to understand how cybersecurity risks translate into business impact assessments and to support informed resource allocation decisions. By using this resource, organizations can mitigate the highest possible risk with the least time and effort required to secure their networks. Investment decisions and expected returns are grounded in risk-based analysis.

Quantitative business risk analysis to support cybersecurity investments, and documented business cases that employ well-established risk quantification methodologies with sound ROI calculations, need to be implemented (Freund & Jones, 2014; FAIR Institute, 2024). When implemented, cybersecurity investments are assessed through the same scrutiny process used to assess other business investments, and resources are directed to initiatives that minimize risk most effectively (and cost-effectively). It requires companies to possess advanced risk-quantification capabilities to translate cybersecurity risk into financial terms and to enable a comparative review of alternative investment options, thereby supporting risk-based investment analysis. This capability enables businesses to make informed decisions about cybersecurity investments. Its goal is, first, to reduce risk; second, to reduce costs; and, very importantly, to align with business objectives.

Flexible funding and emergency response capabilities

Emergency funding for cyber risks enables organizations to respond rapidly to imminent threats or vulnerabilities through a documented escalation procedure, while accounting for the dynamic

nature of the threat landscape (NIST, 2024; Deloitte, 2023). This infrastructure enables organizations to respond promptly to attacks. It is not constrained by traditional budgeting and procurement processes, which are overly time-consuming relative to the response velocity of threats. For organizations to plan for these flexible funding mechanisms, they need to implement risk assessment and escalation processes that can quickly evaluate emerging threats and ensure timely responses. This function enables enterprises to respond efficiently to new, rapidly evolving threats that were not anticipated in regular planning cycles.

2.4. Cybersecurity awareness and training

2.4.1. Cybersecurity awareness

Cybersecurity Awareness (CSA) refers to the cognitive and cultural dimensions in which staff are highly aware of potential cyber threats and actively protect the organization's assets. It is the result of effective communication, leadership, and formal training within the organization. In the Swiss context, establishing a strong security culture through awareness is a primary goal of the National Cybersecurity Strategy 2023–2027 (Federal Council, 2023) and a control area under the NCSC ICT Minimum Standard (Federal Office for National Economic Supply, 2023). Although related to training, awareness is distinct: it is the end state of knowledge and vigilance, whereas training is the formalized process for developing it.

Continuous awareness and communication

Awareness resources must be embedded in continuous communication cycles and tracked via organizational metrics to ensure universal understanding (Arbanas et al., 2021; Da Veiga & Martins, 2015). This shifts cybersecurity from a periodic training topic to a core organizational value. Moreover, cybersecurity education must be delivered more comprehensively, embedded in continuous communication alongside digital marketing channels. According to this philosophy, it is imperative to make cybersecurity a core organizational value, not something to focus on only during special training. Ensuring consistent communication means organizations must establish specific communication strategies across multiple channels and media to connect with different employee groups. Such capacity is especially critical in larger and/or geographically distributed companies, as traditional training approaches may not always reach most of their staff.

Cultural integration and behavioral change

Cultural integration is achieved by embedding cybersecurity responsibilities into job descriptions, performance appraisals, and employee KPIs (Arbanas et al., 2021; Spears & Barki, 2010). This institutionalizes security as a daily responsibility rather than an optional activity. This method will not only embed the concept in employees' cybersecurity awareness but also make it integral to everyday activities, rather than an add-on or optional activity. To achieve cultural integration, organizations implement system-based change management processes that can shift their thinking and behavior. As cybersecurity has become an increasingly prominent topic of conversation in the business world, long-term leadership commitment is needed to implement a rewards-and-recognition process that drives cybersecurity behaviors and behavior change.

Incident reporting and culture development

A "no-blame" reporting culture encourages employees to voluntarily report incidents and "near misses," providing valuable data for organizational learning (Ahmad et al., 2020; ISO, 2022c). This should serve not only educational purposes but also to enhance the effectiveness of cybersecurity. An effective incident-reporting culture depends on complex incident management systems that are both accountable and voluntary. This feature enables organizations to share lessons learned from incidents and near misses to prevent future incidents while maintaining employee involvement and trust.

Leadership commitment and strategic support

Senior management must visibly commit to cybersecurity by communicating regularly about its strategic importance, ensuring realistic budget planning, and actively participating in security exercises (Rothrock et al., 2018; Arbanas et al., 2021). That level of leadership commitment is essential in developing an organizational culture that integrates cybersecurity into day-to-day business operations (Deloitte, 2023). Such leadership commitment is key to building an organizational culture that embeds cybersecurity into day-to-day business operations and inspires employees to participate in awareness-raising efforts.

Senior-level executives must actively engage in cybersecurity and communicate regularly about its importance to the company's success in securing buy-in. It frames cybersecurity as a strategic issue rather than a purely technical one, thereby enabling more effective awareness and cultural

change programs. To secure leadership support, senior-level executives need to engage in cybersecurity actively and frequently articulate its importance to the company's success.

Behavioral monitoring and anomaly detection

Security behavior monitoring, combined with user activity analytics and documented anomaly detection, can also help identify potential insider threats and ensure the organization strikes a healthy balance between privacy and security (He & Zhang, 2019; Arbanas et al., 2021). This will necessitate the establishment of highly flexible systems with robust monitoring, so that abnormalities in any behavior can be detected in depth without causing serious privacy concerns or employee protests. Effective behavioral monitoring should include clear policies and procedures that define appropriate monitoring activities and privacy rights, thereby upholding employee privacy. It enables companies to monitor potential security vulnerabilities with minimal impact on employee trust and participation in security initiatives.

Development and evolution of programs

Security awareness programs must be iterative, using threat intelligence and employee feedback to identify and address deficiencies (Ahmad et al., 2020; Arbanas et al., 2021). As threat landscapes and organizational needs change, this approach ensures that awareness programs remain current. To conduct continuous improvement effectively, organizations need to provide well-designed feedback and evaluation systems that identify where programs may not be working toward their desired goals and how to address those deficiencies. This feature allows organizations to continue making awareness programs work amid dynamic demands and threat landscapes. Security awareness engagement strategies must include approaches and incentives that encourage employees to participate in security-related programs and knowledge-sharing activities actively (Alshaikh, 2020; Arbanas et al., 2021). Organizations must therefore decide not only to enable employees to volunteer (or at least to feel compelled to do so), but also to comply with mandated requirements.

2.4.2. Cybersecurity training

Cybersecurity Training (CST) is defined as formal, structured instruction that develops specific, measurable cybersecurity skills and competencies for employees. It consists of a systematic process involving a defined curriculum, role-based learning objectives, and practical exercises. While awareness is the desired cognitive end-state, training is the formal educational pathway to achieve it through instruction and skill validation (Chowdhury et al., 2022; Hatzivasilis et

al., 2020; Paulsen et al., 2012). Effective training under the Swiss framework is one of the key controls identified in the NCSC ICT Minimum Standard (Federal Office for National Economic Supply, 2023) and the basis for the skills required to implement the National Cybersecurity Strategy 2023–2027 (Federal Council, 2023). Unlike the broader outcome of awareness, training is a precise, targeted intervention aimed at building demonstrable capabilities, whether in technical capacity for IT staff or in securing safe work practices for the rest of the workforce. Effective programs must also be designed for Switzerland's multilingual and culturally diverse workforce so that knowledge is not merely transferred but is transformed into validated competencies.

Role-based training curriculum development

Role-based training curricula should be applied across all employee populations, including the general workforce, privileged users, and software developers, using relevant NIST NICE Framework principles to facilitate cross-organizational role-based training efforts (Paulsen et al., 2012; Hatzivasilis et al., 2020). This method will ensure that the training content is tailored to specific job roles and risk levels, thereby facilitating better skill acquisition and behavior change. The nature of role-based training enables organizations to identify job-specific cybersecurity requirements for specific roles and to design tailored training content to meet these needs through systematic job analyses. This feature enables organizations to focus their training investments on the most relevant skills and knowledge for each employee population.

Training regularity and consistency

At all times during their employment, all employees should receive consistent baseline training, with regular refresher sessions available throughout the enterprise (Paulsen et al., 2012; Hatzivasilis et al., 2020). Regular training ensures staff remain current on threats; however, this requires automated management systems to monitor adherence and minimize administrative burdens (Hatzivasilis et al., 2020). This function helps ensure that training requirements are enforced consistently across the hierarchy, minimizing administrative burden for both training staff and employees.

Risk coverage and threat-specific training

Training focuses on core organizational information security risks, such as phishing campaigns, social engineering, and secure information handling, in accordance with accepted standards and models, including the NIST NICE Framework (Paulsen et al., 2012) and established security

awareness frameworks (Arbanas et al., 2021). This coverage will help employees become aware of, and effectively identify and address, the most common and serious threats they encounter in their workplaces. Organizations must systematically assess threats to design targeted training for specific employee segments, ensuring comprehensive coverage of the most significant risks. Training programs should align with competency frameworks (e.g., NIST NICE) to ensure they meet specific goals. Effectiveness must be validated through pre- and post-training assessments to identify skill gaps (Paulsen et al., 2012; Chowdhury et al., 2022).

Specialized technical training services

Technical staff and related specialized training programs must be appropriately funded to meet budget and aligned with specific framework work roles, which are the functional responsibilities of framework personnel. This should complement training offerings within a professional security program and cover the higher-level technical expertise required of cybersecurity professionals, with training materials that are current with technology.

Simulation-based learning and practical exercises

Incident response teams are regularly required to conduct simulated scenarios and tabletop exercises of varying complexity to maintain preparedness (Hatzivasilis et al., 2020; NIST, 2024). These exercises provide practical training in applying cybersecurity expertise and skills in real-world settings. With that experience, cybersecurity professionals gain more valuable information and develop new skills than they would from traditional classroom-based training. Effective simulation-based learning requires organizations to build advanced exercise design systems that create realistic simulations and deliver meaningful experiences. The ability to test and enhance incident response capabilities enables organizations to create valuable training opportunities for cybersecurity staff.

Competency assessment and validation

Training effectiveness is validated through formal mechanisms that measure and manage cybersecurity skill levels against established standards, with periodic audits and documented corrective actions (Paulsen et al., 2012; Chowdhury et al., 2022). This assessment measures whether the training is being implemented and whether workers are acquiring the competencies necessary for successful cybersecurity performance.

Training effectiveness measurement

Measuring the impact of training and learning effectiveness requires knowledge retention metrics, behavior-change metrics, and concrete evidence that the security posture has improved (Chowdhury et al., 2022; Arbanas et al., 2021). Such a measurement approach ensures that learning programs are assessed by their actual impact on organizational cybersecurity effectiveness, rather than solely on end-user success rates or participant satisfaction. Effective measurement of training quality depends on organizations developing complex data-collection and analysis systems that monitor multiple metrics of program effectiveness over time. This feature enables companies to demonstrate their investment in training and continually improve the effectiveness of their programs.

Program evolution and continuous improvement

The training programs need to be regularly updated, tested, and reviewed, which require assessing emerging threats, implementing technologies, and tracking the evolution of practice. This ongoing enhancement ensures that the training content remains relevant and aligned with the evolving cybersecurity environment, requirements, and risks. A robust process for program evolution involves institutions establishing consistent procedures for reviewing and revising training content, determining when modifications are needed, and promptly implementing them. This feature enables organizations to maintain strong training programs over multiple years, adapting to changing needs and emerging threats.

2.5. Cybersecurity alliance and collaboration

The Swiss National Cybersecurity Strategy 2023-2027 includes public-private partnerships and joint defense mechanisms as essential components of national cyber resilience (Federal Council, 2023). Such strategic direction reflects a shift in the information security governance landscape, as many organizational paradigms are ill-suited to address evolving threats. Cybersecurity partnerships span a range of dimensions, from industry engagement through ISACs to government partnerships with national cybersecurity authorities, academic research and development, and supply chain security coordination.

These collaborative structures are not merely adjuncts to organizational security measures; they constitute part of the fabric of cybersecurity resilience through the sharing of threat intelligence and cooperation on response capabilities, collectively improving the security posture of all actors participating in these efforts (European Union Agency for Network and Information

Security, 2018). Institutional collaboration in cybersecurity is justified by the interconnectedness of digital infrastructure and by the recognition that cyber threats pose systemic risks that require protection. Organizations with complex digital ecosystems face threats originating from multiple vectors that propagate across organizational boundaries. Formal and informal networks within the cybersecurity community share information about emerging threats, attack methodologies, and defensive countermeasures. Active participants in these networks can gain such threat intelligence, which would otherwise be prohibitively expensive or impossible to develop independently. Also, collaborative defense mechanisms have network effects that enhance the overall security posture of all involved entities (European Union Agency for Network and Information Security, 2018).

Institutional participation in industry structures

Effective cybersecurity partnerships require active engagement with established industry structures. Institutional frameworks demonstrate a commitment to collaborative security by maintaining leadership or contributing roles in relevant ISACs aligned with their geographic and sectoral contexts. In the Swiss operational context, this engagement ought to be documented through participation records, meeting attendance, and substantive contributions to ISAC activities (European Union Agency for Network and Information Security, 2018; Federal Council, 2023). The ISAC model provides formalized mechanisms for threat information exchange, vulnerability disclosure coordination, and collective response to emerging threats. In their ISAC-led efforts, organizations demonstrate a strong commitment to an integrated security ecosystem, serving as cornerstones that shape industry standards and practices.

Through ISAC participation, enterprises also establish formal ties with relevant regional and national cybersecurity authorities. In the Swiss context, this might include engaging directly with the Swiss National Cyber Security Centre, the country's central government cybersecurity office. These relationships are enshrined in a formal cooperation framework that outlines how information sharing, incident reporting, and crisis management protocols ought to be managed (Federal Council, 2023).

Academic collaborations are a third dimension of institutional cooperation. Companies collaborate with academic research and development bodies in Switzerland and neighboring countries on cybersecurity. These partnerships provide various benefits, including access to state-of-the-art research on emerging threats and defensive technologies, opportunities for

educational collaborations to develop cybersecurity talent, and opportunities for organizations to contribute to advancing cybersecurity science (European Union Agency for Network and Information Security, 2018; Federal Council, 2023). Documented collaborative activities might include research projects, curriculum development, student internship programs, or participation in academic conferences and working groups. These activities create bidirectional knowledge flows that enhance both organizational security capabilities and the quality of academic research.

Participation in industry-wide initiatives

The timely exchange of information largely determines the performance of cybersecurity partnerships. Organizations engaged in mature cybersecurity collaboration share mutual risk through reciprocal actions, including bidirectional threat information sharing with industry entities and government agencies. These entities share information through formal processes under sharing arrangements and documented procedures that detail the types of information shared, classification levels, and allowable uses (European Union Agency for Network and Information Security, 2018; Federal Council, 2023). Bidirectional sharing is distinct from unidirectional information exchange and distinguishes mature and non-mature collaborative relations from the typical two-way channel, in which organizations share information about threats from their own security monitoring and receive intelligence from third-party members.

International collaboration requires navigating between threat sharing and Swiss data sovereignty. The trade-off between sharing information and safeguarding personal data is particularly pronounced in Switzerland, where neutrality and data protection are constitutional principles that shape all forms of international cooperation. Organizations must establish legal and technical frameworks to share intelligence while upholding privacy and neutrality (Federal Council, 2023).

Supply chain collaboration is vital for standardizing security postures and complying with the EU NIS2 Directive, as attacks often propagate through compromised third-party providers (European Commission, 2023; NIST, 2024). Collaboration in the supply chain is more than simply aligning suppliers; it encompasses shared threat intelligence, incident response, and security collaboration. An important aspect of this focus on supply chain security is that cyberattacks can spread across multiple organizations via compromised providers or suppliers.

The maturity of cybersecurity collaboration in standards development and best-practice initiatives within industry associations is the last dimension of mature cybersecurity cooperation. Participation in standards development organizations and industry working groups also helps shape cybersecurity standards (Federal Council, 2023). This participation helps ensure that companies' security practices meet new or emerging industry standards and gain influence in shaping standards that translate into practice as businesses and practitioners conduct their business. Professional organizations and industry associations share best practices to accelerate the adoption of robust security measures across the industry, thereby enhancing the security posture for all stakeholders.

2.6. Cybersecurity top management risk perception and support

2.6.1. Cybersecurity top management risk perception

According to the COSO Enterprise Risk Management Framework, a strong risk culture and governance structure are foundational elements of effective enterprise risk management (COSO, 2017). For a cybersecurity organization, risk perception is the extent to which senior leaders understand the cyber threat landscape and its potential impact on the organization's objectives. At its core, successful information security governance is rooted in alignment between the perception of cyber risks at the top of the hierarchy and the technical analyses in practice. Alignment is achieved through documented risk communication processes and regular reviews to establish a common understanding of the organization's risk posture (COSO, 2017; ISO, 2018).

Alignment mechanisms and communication channels include risk briefings by security professionals to senior management, documented risk assessment methodologies and results, and formal communication processes to demonstrate the implications of recognized risks for strategy and organizational operations (COSO, 2017; NIST, 2024). These mechanisms also provide leadership with clarity and knowledge, including not only which risks have been identified but also the methodologies used to assess risk severity and likelihood, which are required for risk acceptance or mitigation.

Systems thinking and interconnected risk assessment

Modern cyber risk assessment requires systematic thinking, considering the connections between risks and the capacity of failures to propagate across different parts of the organization. Cyber risk is not isolated; leadership must know that the operational, financial, reputational,

and strategic risks of cybersecurity are also interlinked (ISO, 2018; COSO, 2017). This all-encompassing approach is supported by well-documented risk-scenario analyses and strategic planning exercises that examine the ramifications of cyber incidents and how they can ripple through organizational systems and supply chains. Systems thinking recognizes that cyber risks are interconnected; breaches in supply chains can cause cascading failures. Therefore, risk assessments must include supply chain management and business continuity functions.

Structured decision-making and bias mitigation

Cognitive studies reveal systematic biases in human judgment that distort risk assessment, leading to suboptimal decisions (Kahneman, 2011). To ensure objective risk evaluation, organizations should use structured decision-making and bias-mitigation techniques, such as red-team exercises, to challenge prevailing assumptions (Kahneman, 2011; Lovallo & Sibony, 2010). Using bias-mitigation methodologies in cybersecurity risk assessments makes the assessment more objective and improves its quality. In this way, organizations that recognize cognitive biases in their assessment processes and adopt systematic methods to identify and remediate them produce better risk assessments and higher-quality risk decisions. Documenting bias-mitigating techniques provides evidence that risk assessment processes include systematic steps that help make them more objective.

Threat awareness and intelligence use

Senior leaders need to remain attuned to the rapidly evolving cyber threat landscape and its impact on organizational security. A high level of awareness is developed through a well-defined briefing that covers the cyber threat landscape, identifies organizational weaknesses, and outlines potential impacts (COSO, 2017; Dal Cin et al., 2025). These briefings should be held regularly and should include written action items that translate awareness of the threat into organizational impact.

Threat intelligence should be strategically integrated into business decision-making. Institutional structures reflect a mature risk mindset, in which threat intelligence informs strategic business decisions across departments (Dal Cin et al., 2025). This interlink ensures that cybersecurity needs are integrated into business processes and decisions, rather than addressed only after decisions have been made. Senior leaders stay current with the latest threats by attending and participating in external cybersecurity events and forums. Moreover, external engagement generates a repository of emerging threat insights, industry best practices, and

security experts' views across groups, industries, and sectors (Deloitte, 2023; Dal Cin et al., 2025). External engagement enhances leadership's understanding of the existing threat landscape and offers opportunities to learn from peer organizations.

Risk-informed decision making

An organization with a mature risk perception can show a risk-informed decision-making process, embedding the best-documented cyber risk analysis from assessment and analysis into key decisions. Formal assessment of cybersecurity risks, including cost-benefit analyses of security investments, should inform significant business decisions (Gordon & Loeb, 2002; COSO, 2017). This ensures that cybersecurity considerations are mainstreamed into business decision-making rather than treated as a bolt-on afterthought. Institutional frameworks also demonstrate mature risk-informed decision-making, as evidenced by documented cases in which projects were rejected or halted due to unacceptable associated cyber risks (COSO, 2017; NIST, 2024).

Mature risk-informed decision-making is evident when leadership is willing to forgo commercial opportunities because of unacceptable cyber risks. Scenario-oriented planning exercises can inform and guide top-down decision-making. Leaders gain an intuitive understanding of the threats posed by organizational weaknesses and how anticipated business impacts of a cyber incident may affect operations. In this realm, exercises involve considering multiple severe but plausible cyber scenarios, including worst-case scenarios, and possible organizational responses to these threats (National Association of Corporate Directors, 2023). Through exposure to realistic cyber scenarios and a greater focus on proactive risk management, leadership will be more effective at recognizing organizational risk.

2.6.2. Cybersecurity top management support

Effective cybersecurity governance depends on visible and sustained commitment from organizational leadership (Rothrock et al., 2018; National Association of Corporate Directors, 2023; NIST, 2024). This commitment takes the form of strategically aligning cybersecurity priorities with the overall business strategy, preserving cybersecurity budgets amid financial constraints, and publicizing cybersecurity as an enabler of business rather than a cost center. Similarly, cybersecurity governance frameworks underscore the need for boards to engage with and align on strategic objectives to manage cybersecurity effectively (NIST, 2024; National Association of Corporate Directors, 2023).

For strategic alignment, security staff should conduct an annual review of the organization's cybersecurity strategy to ensure it remains aligned with evolving business objectives. In this way, board approval and documented assessment methods demonstrate a direct correlation between cybersecurity investments and business objectives (NIST, 2024; National Association of Corporate Directors, 2023). The annual review process serves three purposes: first, it keeps cybersecurity strategies aligned with changing business environments; second, it provides leadership with an opportunity to reassess their cybersecurity priorities in light of new threats or business developments; and third, it creates a formal record documenting strategic alignment for future board governance considerations.

Organizations with mature cybersecurity governance increasingly position cybersecurity as a strategic business enabler rather than a cost center, thereby helping to justify sustained investment even during cost-reduction periods (Deloitte, 2023). This safeguard stems from the understanding that cybersecurity funds will yield long-term benefits (in terms of risk reduction and operational resilience) rather than being treated as discretionary during financial crunches. Leadership advocacy positions cybersecurity as a business enabler, ensuring budget protection even during financial constraints (Rothrock et al., 2018). Such advocacy is evidenced by documented communications with internal stakeholders, participation in cybersecurity awareness initiatives, and engagement with external stakeholders regarding organizational security practices. To this end, leadership advocacy helps foster an organizational culture that promotes security and encourages employee buy-in to security practices.

Governance structures and oversight mechanisms

The development of effective information security governance relies heavily on organizational structures that ensure that cybersecurity concerns receive appropriate engagement at the highest levels of organizational decision-making. Board-level risk committees will need to include members with technical cybersecurity expertise or sufficient education to conduct informed cybersecurity risk assessments (Rothrock et al., 2018; National Association of Corporate Directors, 2023). This expertise can be obtained through formal certifications, such as the Certified Information Systems Security Professional or the Certified Information Security Manager, or through extensive professional experience in cybersecurity roles (Rothrock et al., 2018; Burch et al., 2024). Ensuring cybersecurity expertise at the board level ensures that digital security vulnerabilities are appropriately considered alongside other enterprise risks and

enables meaningful board-level governance discussions of cybersecurity strategy and risk management.

The Chief Information Security Officer (CISO) governance model establishes organizational structures to ensure the CISO has sufficient authority and access to senior leadership. A CISO should hold a senior-level or C-suite position with well-defined reporting lines and regular access to the board or risk committee (Rothrock et al., 2018; Burch et al., 2024). It ensures that cybersecurity threats are elevated to executive decision-making levels and provides the CISO sufficient authority to implement security strategies. Regular access to the board or the risk committee enables the CISO to communicate threat updates, security incidents, and resource needs to senior stakeholders.

Performance accountability mechanisms embed cybersecurity performance factors into senior executive accountability frameworks with established Key Performance Indicators (KPIs) and performance measurement systems (ISO, 2016; Gartner, 2023). When combined with executive compensation and performance review mechanisms, cybersecurity outcomes serve as a compelling catalyst for leaders to prioritize investment in security projects. Documenting performance metrics clearly shows how cybersecurity performance is measured and evaluated within the organization.

Accountability and performance management

Accountability for organizational cybersecurity effectiveness and performance should not be limited to senior leadership; it should also include business unit leaders and operational managers. Cybersecurity performance should be reported systematically to the board through structured, metric-based dashboards that provide extensive information, including KPIs and Key Risk Indicators (KRIs) (ISO, 2016; National Association of Corporate Directors, 2023). Data dashboards like these provide board members with detailed statistics on how their company manages security, including controls against potential threats, whether operations are functioning as intended, and whether new threats require additional resources or attention. A formal governance model holds business units accountable for digital security vulnerabilities: business unit leaders manage them within their areas of responsibility. This model must be documented in terms of roles and responsibilities that specify which security functions fall under which domain and to what extent and include periodic performance measurement against established metrics (Putrus, 2019; NIST, 2024). Accountability within a business unit makes cybersecurity as integral to overall operations as specialized security functions.

The accountability instruments should be supplemented by appropriate delegation of authority and allocation of resources. Cybersecurity accountability and responsibility require more than clearly defined roles and responsibilities; they require that appropriate levels of authority be delegated to individuals responsible for cybersecurity functions and that sufficient resources be allocated to enable the successful execution of cybersecurity responsibilities. This principle is codified in sector-specific regulations such as DORA for the financial sector (European Parliament and Council of the European Union, 2022a). It is reflected in broader governance frameworks (NIST, 2024). Documentation demonstrating delegation of authority and adequate resource allocation indicates that accountability mechanisms are supported by the organizational infrastructure necessary for their successful implementation.

2.7. External factors: market and technological turbulence

2.7.1. Market turbulence

Market Turbulence (MT) is a dynamic environment characterized by rapid, often unpredictable shifts in customer behavior, competitive dynamics, regulatory requirements, and macroeconomic factors. Such changes increase uncertainty and require organizations to allocate resources to adapt and respond strategically (Durst et al., 2024; Liu et al., 2024). International economic rules, global business linkages, and Switzerland as an international financial center play a central role in market turbulence in Switzerland (Federal Council, 2023; FINMA, 2022; Rentsch et al., 2017). In such an environment, institutions with a mandate to continuously monitor market conditions, respond strategically to new opportunities, and defend against new threats would benefit from developing capabilities. Market turbulence relates to cybersecurity maturity through the shared understanding that market volatility heightens existing security vulnerabilities and amplifies new security threats. Organizations that are quickly reinventing their business models, entering new markets, or adopting new models could introduce new security vulnerabilities. In addition, market turmoil may tempt organizations' senior leaders to shift attention from cybersecurity to other priorities, thereby forcing them to adopt technologies without appropriate security assessments. This means institutions in volatile markets must remain highly aware of digital security vulnerabilities when evaluating opportunities and risks.

Market monitoring and strategic response

A systematic market monitoring and strategic response approach is necessary for institutional entities facing unpredictable, rapidly changing market forces. Frequent tracking of market

volatility cues, such as changes in customer demand, the emergence of new competitive forces, and regulatory reforms, provides a basis for designing strategic response plans (Durst et al., 2024). Such monitoring should be based on market analysis and the formulation of strategic response plans, including how the organization would respond to observed market changes. Enterprises should create written procedures for responding to large-scale market disruptions to document how the organization will approach them (Elliott & Swartz, 2010). Businesses must continually monitor their competitors, emerging competitors, technological developments, and business model disruptors, as these factors can shape the competitive environment. Strategic decisions on how to position a product in the market, develop a competitive product, or invest are guided by such competitive intelligence. It is important for institutional entities in regulated industries or operating across multiple jurisdictions to monitor regulatory changes and compliance requirements in each jurisdiction continuously. This monitoring should be accompanied by documentation of regulatory impacts, including an adaptation plan, to ensure that the organization remains aligned with evolving regulations (Federal Assembly of the Swiss Confederation, 2023; FINMA, 2022). Regulatory compliance is particularly crucial in Switzerland, where institutions are subject to stringent regulations governing the processing of personal data.

Competitive threat assessment and market disruption

Institutions facing frequent and significant competitive threats should conduct ongoing competitive threat analysis that includes assessments of new entrants, disruptive technologies, and shifts in consumer preferences. This analysis should be supported by documented plans for threat assessment and response that detail how the company will address competitive threats (Porter, 1985). Competitive threat analysis assesses not only current competitors but also potential market entrants and disruptive business models that may transform competitive dynamics. There is a need to proactively prepare for market disruptions through scenario planning, contingency planning, and adaptive strategies. These capabilities enable businesses to respond quickly to disruptions rather than remain unprepared for market changes. Increased innovation across all types exerts pressure on organizations to adopt new technologies to remain competitive. These pressures for innovation require clearly defined innovation strategies and implementation plans that balance the potential benefits of new technologies with their associated risks and costs (Rogers, 2003). Enterprises need to develop the capability to analyze emerging technologies, assess their competitiveness, and make informed decisions regarding timeframes and implementation approaches.

Stakeholder management and conflicting demands

Regulators, customers, investors, and workers often have external demands on organizations. These disparate stakeholders create tension in organizational decision-making. Stakeholder theory emphasizes the interdependence of stakeholders and the need to balance fairness and value creation across the stakeholder system (Freeman et al., 2020). In this study, these principles are operationalized through documented stakeholder analysis, prioritization, negotiation, and conflict-resolution procedures. Such processes would comprise premeditated matrices that explicitly weigh the parties' diverse interests, negotiation protocols that mediate conflict, and decision-making processes that allow conflicting interests to be rationally considered publicly by all parties. The primary friction point may be the relationship between business and regulatory requirements. It is therefore incumbent upon organizations to develop written compliance plans that detail how the regulations will be met and the business objectives to be achieved. At this point, compliance and risk–benefit analyses should be carried out to compare the costs and benefits of different implementation approaches (FINMA, 2022; Federal Council, 2023). The balance between compliance and performance is especially challenging in Switzerland, where strict regulations carry severe penalties for noncompliance.

2.7.2. Technological turbulence

Technological Turbulence (TT) refers to rapid technological change, broad adoption of new technologies, digital transformation pressures, and rapid innovation cycles, both opportunities and threats that technology poses to an organization's digital security (Durst et al., 2024; Tushman & Anderson, 1986). Contemporary technological disruptions include the increasing use of AI in systems, cloud computing, the Internet of Things, and quantum computing. These technological changes require sophisticated risk management and adaptation approaches that align with the NIST Cybersecurity Framework 2.0 (NIST, 2024). They are also addressed by the EU Cyber Resilience Act (European Union, 2024) and the Swiss National Cybersecurity Strategy (Federal Council, 2023).

The linkages between technological turbulence and cybersecurity maturity are grounded in the understanding that new technologies expand an organization's attack surface by introducing additional attack vectors. Institutions that transition to new technologies without a proper security assessment risk inadvertently introducing critical vulnerabilities. Moreover, rapid technological advancement can create gaps in organizational-level security assessment and implementation, relative to the ability to evaluate their capabilities. Thus, institutional actors

operating in fast-paced information technology transformation environments should be more vigilant about detecting digital security threats associated with technology adoption.

Technology monitoring and strategic planning

Institutional actors operating in today's rapidly changing and unpredictable technological environments are called upon to conduct monitoring and make informed decisions about technology strategy. Systematic, integrated trend tracking of emerging technologies that affect organizational functioning should take place alongside technology forecasting, research and development (R&D) project development, and strategic planning (NIST, 2024). This monitoring should identify emerging technologies and services that could threaten the company's competitive advantage or pose additional security risks.

Pressure from digital transformation can be managed only when documented transformation strategies are used, with implementation roadmaps detailing technology adoption management (Rogers, 2003; Liu et al., 2024). Digital transformation strategies are not limited to technology implementation; they must also address organizational transformation, human capital development, and governance to facilitate and sustain the adoption of new technologies. A roadmap for implementation must outline the deadlines, resource requirements, and success criteria for technology adoption projects. This has made it imperative for organizations to adopt disciplined approaches to innovation management and technology lifecycle planning, given shorter iteration and refresh cycles. Businesses should implement existing innovation diffusion frameworks to understand the dynamics of technology adoption and to make informed decisions about the timing and approach to adopting new technologies (Rogers, 2003). These models serve as the basis for examining the impact of new technologies, assessing the optimal timing for adoption, and overseeing the transition to a new platform relative to legacy technologies.

Technology integration and assimilation

Integrating and managing multiple emerging technologies is complex and challenging for many organizations. Enterprises need the capabilities to manage the complexity of technology integration, such as system interoperability, data integration, and architectural coherence; organizations must develop these capabilities to handle this complexity and meet integration demands. These capabilities should also be complemented by documented integration frameworks and governance structures, such as those provided by The Open Group Architecture Framework (The Open Group, 2022). Integration frameworks provide structured

methodologies for assessing technology compatibility, defining integration requirements, and executing the integration project.

Technology assimilation should be a systematic process that involves evaluating new technologies, conducting pilot studies to verify their appropriateness, and documenting the process for scaling such initiatives (Rogers, 2003; NIST, 2024). This structured approach to introducing technologies, however, prevents unnecessary risks associated with unproven technologies and helps embed them effectively within organizations. Strategic fit and integration across a range of initiatives requires dynamic capabilities approach that enables firms to integrate, build, and reconfigure competencies in rapidly changing environments (Teece et al., 1997; Rogers, 2003). Technology portfolio management provides tools for selecting technologies across organizations and a process for determining how to integrate and exclude redundancy and conflicting technologies, in ways that best utilize and balance them, to ensure an overall technology portfolio that supports successful integration and alignment with enterprise strategy.

Competitive technology and security considerations

New technologies have intensified competitive pressure on enterprises to adapt. This pressure should be carefully managed to avoid unacceptable security risks. Enterprises need to develop documented technology adoption frameworks that appropriately balance security and operational risks (Rogers, 2003; NIST, 2024). These frameworks create mechanisms for the rapid adoption of proven technologies and the careful application of unproven or high-risk technologies. However, the need to balance innovation with cybersecurity should be incorporated into the specific decision-making process for technology adoption. Security-by-design principles and risk management should be integrated into the technology adoption processes to ensure responsible innovation (NIST, 2024; European Union, 2024). In security-by-design approaches, security is integrated into technology development and implementation rather than treated as an afterthought.

This second chapter presented a systematic analysis of key constructs characterizing the contemporary cybersecurity landscape. It begins with a foundational definition and then traces the evolution of cybersecurity from a technical domain to a holistic, socio-technical space. Key elements and modern frameworks, such as NIST and ISO, were described, and each main variable in the research model was operationalized in depth, ranging from Cybersecurity Risk Maturity and Technological Infrastructure to human- and environmental-level drivers, such as

Top Management Support and Market Turbulence. This chapter establishes the theoretical and practical foundations for the subsequent empirical investigation, situates each construct within the existing literature and relevant standards, and outlines the context that will be critical to understanding how these constructs are measured and analyzed.

3. CYBER RESILIENCE AS THE BACKBONE OF BUSINESS CONTINUITY

This chapter analyzes how organizations develop the capacity to anticipate, absorb, and recover from cyber incidents. By evaluating BCP paradigms (ISO 22301) and incident response frameworks (NIST SP 800-61), it establishes resilience as a sociotechnical construct driven by technological infrastructure, human competency, and governance maturity.

3.1. Organizational resilience

Organizational resilience is an organization's ability to prepare for, withstand, and adapt to disruptions without compromising its business-critical functions, according to the Swiss National Cybersecurity Strategy 2023-2027 (Federal Council, 2023). The conceptualization complies with the NCSC ICT Minimum Standard (Federal Office for National Economic Supply, 2023). It adheres to the appropriate cybersecurity practices outlined in ISO standards (ISO, 2019). Modern studies also show that organizational resilience has shifted from a reactive crisis-response approach to the proactive development of technical, organizational, and strategic capabilities (Liu et al., 2024; Jiang et al., 2019; Bhamra et al., 2011; Hammer & Champy, 2006). Grounded in Dynamic Capabilities Theory, resilience is defined by an organization's capacity to sense environmental changes, seize opportunities, and transform resources to maintain a competitive advantage during disruptions (Teece et al., 1997; Bhamra et al., 2011). Liu et al.'s recent empirical work (2024) demonstrates that digital orientation is important for organizational resilience and dynamic capabilities. Their examination from 1,875 firms also suggests that dynamic capabilities in turbulent environments are essential for greater responsiveness. This aspect of the cybersecurity environment has become increasingly prevalent, with many organizations continually struggling to adapt while remaining productive (Kraus et al., 2020).

Incident containment and response capabilities

An essential dimension of organizational resilience is effective incident containment, which requires specialized capabilities for threat identification, isolation, and neutralization (NIST, 2024). The Swiss National Cybersecurity Strategy and international incident-management standards emphasize formalized response procedures and incident-specific containment measures (Federal Council, 2023; ISO, 2023). This aligns with the best international practice recommended in NIST SP 800-61r3, which integrates incident detection, response, and

recovery into the CSF 2.0 Respond and Recover Functions (NIST, 2025; Thompson, 2018). To keep pace with ever-evolving threat landscapes, organizations require incident response capabilities, and research shows that well-developed, tested incident response capabilities are essential (Kanaan et al., 2025). Integrating machine learning into resilience frameworks enhances continuity by automating threat detection and adapting remediation processes in response to real-time incident data (Sarker, 2022). With this technical enhancement, enterprises can add advanced detection and response capabilities to an already complex incident response while continuing to perform this work with human resources.

Operational resilience and service delivery continuity

Operational resilience goes beyond mere business continuity; it is the ability of organizations to respond to and recover from disruptions while minimizing impact on service delivery, as supported by business continuity management frameworks (ISO, 2019; Institute of Risk Management, 2021). This is particularly important in regulated environments, where organizations must demonstrate their ability to continue providing critical services even when operations are severely disrupted. Operational resilience can only be achieved and validated through rigorous testing beyond standard disaster recovery exercises. Organizations must validate resilience through rigorous testing of threat scenarios and by measuring performance against specific service-delivery targets to ensure capabilities are executable during actual disruptions. It also ensures that such resilience capabilities are not merely paperwork; they can be implemented during real disruptions.

Adaptive cybersecurity strategy design

Adaptive cybersecurity strategies have evolved to address unexpected threats, and the ability to rapidly revise policies and procedures in response to changes in the threat environment is an essential component of organizational resilience. Adaptive security architecture requires the continuous adjustment of controls based on threat intelligence and risk assessments, supported by formal change-control processes (NIST, 2024; Ahmad et al., 2020), and the documentation of change-control processes to ensure that new security issues are addressed promptly. Being adaptive on these fronts requires organizations to build complex threat intelligence capabilities that can detect emerging threats and translate that intelligence into security actions. Such a fusion of artificial intelligence and machine learning technologies can be crucial for real-time adaptability to evolving threats (Sarker, 2022; Prakash et al., 2024; CISA, 2023a). Evidence

shows that businesses with effective adaptive capabilities are better able to address cyber threats and remain operational during disruptions (Liu et al., 2024; Järveläinen et al., 2025).

Threat response, agility, and dynamic capabilities

Organizations should be able to maintain flexible security architectures that enable the rapid deployment of additional defensive functions without interfering with operational activities (Ahmad et al., 2020; CISA, 2023b). Threat-response agility necessitates organizational sensing of threat conditions and adaptive resource management to deploy defenses without disrupting operational activities (Teece et al., 1997; Järveläinen et al., 2025). Recent empirical work shows that organizations with high dynamic capabilities respond more positively than others to cyber threats over time and maintain operational effectiveness during periods of high threat activity (Liu et al., 2024).

Strategic flexibility in cybersecurity management

Strategic flexibility in cybersecurity management requires organizations to regularly review and update their strategies in response to changing business and threat environments, with senior leadership approval for significant strategic changes (Ahmad et al., 2020; NIST, 2024). This ability helps organizations ensure not only that their cybersecurity plans align with organizational needs and are continuously adjusted to changes in risk and value, but also that these adjustments are documented and tracked over time (Ahmad et al., 2020; NIST, 2024). Strategic adaptability relies on governance mechanisms that balance agile decision-making with structured accountability and performance measurement.

Organizational learning from cybersecurity incidents

Systematically applying lessons learned from cybersecurity incidents to enhance security management is a significant part of organizational resilience. International incident response guidance requires that all cybersecurity incidents include written post-incident review debriefs documenting root cause analysis and lessons learned (NIST, 2025). Evidence of organizational learning effectiveness requires that lessons learned be integrated into revised policies, procedures, and training programs, with documented timelines and proof of implementation (Ahmad et al., 2020; ISO, 2019; Lengnick-Hall et al., 2011). Organizational learning effectiveness is measured by reduced incident recurrence rates and enhanced detection capabilities (NIST, 2024; Ahmad et al., 2020).

Continuous improvement and security posture enhancement

Organizations need to adopt systematic processes for identifying, evaluating, implementing, and analyzing lessons learned, threat intelligence, and performance metrics to support ongoing improvements in security posture. This process enables security functions to evolve rather than remain static, keeping organizations relevant in an ever-changing threat landscape. Continuous improvement can only be measured using complex metrics that combine quantitative performance metrics with qualitative perspectives on the evolution of security capabilities. Organizations need to build balanced scorecards that capture the several ways security performance can be evaluated and inform continuous improvement strategies (NIST, 2024; CISA, 2023a).

Integration of resilience capabilities with business strategy

Incorporating resilience capabilities into broader business strategies means that cybersecurity projects become not just cost centers in the organization but levers for improving performance rather than constraints. Integrating it into an organization will require the involvement of senior leaders and new governance approaches that balance security needs with organizational goals. For resilience to align with the business strategy, organizations would require complex risk management frameworks that account for cyber risks and translate them into business impact assessments that influence strategic decisions. This is enabled by firms' ability to make rational investments in resilience capabilities that will allow them to achieve the best risk-reduction rate at a cost (and complexity) commensurate with the cost of obtaining it.

3.2. Business continuity

Business continuity comprises interrelated factors that support an organization's survival and adaptation during disruptive events while preserving vital tasks and stakeholder relationships (Sahebjamnia et al., 2015). Modern literature makes it clear that successful business continuity requires integrating strategic, operational, and tactical business, each of which constitutes a fundamental capability for readiness, response, recovery, and learning (Herbane, 2010a; Gibb & Buchanan, 2006; Bajgorić et al., 2013; Spremić et al., 2018). The element-based approach to business continuity recognizes that organizational resilience is the inevitable outcome of the interplay among systems and capabilities, rather than being isolated from any given process or technology (Herbane, 2010a; Sahebjamnia et al., 2015). Business continuity strategic components reflect the governance structures, policy frameworks, and resource allocation

mechanisms through which continuity planning and practice provide both direction and support (McManus et al., 2008; Burnard & Bhamra, 2011). Organizations should have a clear policy and procedure framework to ensure continuity is the focus of all business activities. This encompasses executive leadership and board oversight that establishes an organizational culture of engagement with a mission to ensure continuity (Gibb & Buchanan, 2006; Lindström et al., 2010). However, contemporary frameworks underscore the need to integrate business continuity with the broader plan and governance system to better align with business goals and stakeholder expectations (Business Continuity Institute, 2024; Elliott & Swartz, 2010).

Risk assessment and business impact analysis are core strategic dimensions that facilitate organizations to assess their susceptibility to disruptions and determine where to invest in continuity (Sahebjamnia et al., 2015; Herbane, 2010a). Modern-day risk assessment for business continuity focuses on holistic threat assessment, vulnerability analysis, and impact measurement, and addresses traditional hazards and emerging risks such as cyber risk, supply chain disruption, and pandemic events (Business Continuity Institute, 2024; Elliott & Swartz, 2010). Dynamic risk assessment capabilities that can adjust to evolving threat landscapes have become a prerequisite for sustaining effective continuity planning over the long term (Sahebjamnia et al., 2018). Operational aspects of business continuity are the processes, procedures, and capabilities that enable organizations to continue operating during a disruption (Bhamra et al., 2011; Burnard & Bhamra, 2011). These components can include Business Process documentation and analysis to identify critical processes and dependencies, Alternative operating procedures to maintain operations at low levels of functioning, and Resource Management systems to monitor available staff, facilities, and technologies (Linkov & Kott, 2018; Dupont, 2019).

Technology and infrastructure components form the technical foundation of business continuity, ensuring that essential systems and data are maintained during disruptive events (Elliott & Swartz, 2010; Business Continuity Institute, 2024). These include backup and recovery systems that protect against data loss and system failures, alternative communication and collaboration platforms that enable remote work and distributed operations, and redundant infrastructure that supports alternative paths for critical operations (Elliott & Swartz, 2010; Sahebjamnia et al., 2018). Cloud computing, mobile technologies, and artificial intelligence have enabled new approaches to technology use in business continuity, enabling it to adapt and scale up (Sarker, 2022; Prakash et al., 2024). The realization of integrated, scalable technology systems is a key dimension of an organization's technological structure and underpins

cybersecurity risk maturity (Aldea et al., 2023). Integrated systems are defined as the seamless, interconnectedness of heterogeneous technological elements that deliver unified data flows and coordinated security protocols (NIST, 2024; Aldea et al., 2023). In fact, scalability refers to an organization's capacity to adapt to varying operational needs and threat environments (Malatji et al., 2022).

Strategic integration and scalability enable agile, scalable defense mechanisms (NIST, 2024). In the evolving cybersecurity landscape, mature risk management processes emphasize the need for modular, interoperable infrastructure that enables 24/7 monitoring and rapid threat detection (CISA, 2023b). The human resources dimension recognizes that business continuity ultimately depends on the knowledge, skills, and commitment of an organization's people (Lengnick-Hall et al., 2011; Business Continuity Institute, 2024). These components include succession planning and cross-training initiatives responsible for ensuring the availability of personnel for critical activities; emergency communication and coordination strategies that maintain effective decision-making during periods of disturbances; and support and welfare initiatives that ensure employees are engaged and motivated to work actively in times of difficulties (Federal Emergency Management Agency, 2018; Business Continuity Institute, 2024).

Current human resources strategies for business continuity emphasize cultivating organizational culture and values that promote resilience-building behaviors and attitudes (Lengnick-Hall et al., 2011; Bhamra et al., 2011). Supply chain and stakeholder components relate to the external dependencies and relationships that are fundamental to an organization's operations (Business Continuity Institute, 2024; ISO, 2022b). These consist of supplier diversification and qualification systems reducing reliance on a single source for essential commodities and services, customer communication and service continuity plans that help nurture customer relations in the wake of business disruption, and stakeholder engagement and coordination systems that promote collaborative solutions to shared problems (European Commission, 2023; European Parliament and Council of the European Union, 2022a). Establishing ecosystem-wide continuity competencies is important for addressing the interconnectedness of modern businesses (Federal Council, 2023; FINMA, 2024). Research shows that financial planning for business continuity necessitates a very complex methodology that addresses the direct and indirect impacts of disruption and loss response (Gordon & Loeb, 2002; Gordon et al., 2016).

However, the components of testing and validation help to evaluate and improve business continuity capacity through regular procedures and tests (Herbane, 2010a; Gibb & Buchanan, 2006). Tabletop exercises and simulations are crucial for understanding decision-making and coordination; functional tests to assess specific continuity processes or technology-enhanced continuity activities; and full-scale exercises for evaluating organizational response mechanisms (Business Continuity Institute, 2024; Herbane, 2010a). In particular, reliable and structured test programs have become a basic prerequisite to the successful implementation and timeliness of continuity plans (McManus et al., 2008; Burnard & Bhamra, 2011).

Continuous improvement helps ensure that business continuity capabilities remain up to date, so that lessons learned from exercises and real-life situations are used and adapted in organizational transformations and the transformation process (Gibb & Buchanan, 2006; Lindström et al., 2010). Post-event analysis and lessons-learned processes (Ahmad et al., 2020; Herbane, 2010a) identify gaps for improvement; performance measurement and monitoring systems track the effectiveness of continuity; and maintenance/update procedures ensure retention and relevance. Creating learning-based continuity capabilities that are responsive to temporal change is an ongoing theme in modern paradigms (Burnard & Bhamra, 2011; Lindström et al., 2010).

Relationship with risk management

The link between business continuity and risk management is central, encompassing both theoretical and empirical aspects, which have developed significantly as organizations have come to recognize mutually supportive yet sometimes divergent roles for these approaches in organizational resilience (Elliott & Swartz, 2010; Herbane, 2010a). Several studies have delineated that business continuity and risk management have two aspects: the first addresses risk recognition, risk assessment, and risk control, whilst the second emphasizes the continuity of critical operations and the recovery of operations when risk management strategies prove insufficient (Elliott & Swartz, 2010; Sahebjamnia et al., 2015). Risk management and business continuity strategies were integrated to form an overall set of organizational defenses against threats (Business Continuity Institute, 2024; ISO, 2022b).

There are meaningful conceptual differences between risk management and business continuity: risk management employs threat-based activities to reduce or eliminate the likelihood and impact of threats, whereas business continuity focuses on remediation measures to maintain critical processes during a disruption (Elliott & Swartz, 2010; Herbane, 2010a).

Contemporary practice considers both essential and compatible: risk management to identify and control threats, and business continuity, to maintain operations when risk management is unsatisfactory (Business Continuity Institute, 2024; ISO, 2022b). Time is the distinguishing factor between risk management and business continuity: risk management involves analyzing threats and implementing prevention measures, whereas business continuity encompasses readiness and recovery operations (Sahebjamnia et al., 2015; Sahebjamnia et al., 2018). Achieving organizational resilience requires integrating multiple time horizons: risk management provides continuous monitoring and mitigation capabilities, while business continuity provides strategic and operational capabilities to withstand disruptions (Federal Council, 2023; FINMA, 2024; Sahebjamnia et al., 2018). Multi-time-resilient systems must be implemented to address the short- and long-term continuity imperatives of threats (FINMA, 2024). Scope and coverage differences between risk management and business continuity stem from distinct objectives and methods: risk management typically focuses on specific threats and vulnerabilities that can be detected and quantified, whereas business continuity typically focuses on broader threats and vulnerabilities that may not be detectable or quantifiable.

Modern business frameworks recognize that many disruptive events cannot be anticipated or prevented through conventional risk management methods; thus, there is a need for business continuity capabilities that respond to unknown situations and novel challenges (McManus et al., 2008; Burnard & Bhamra, 2011). Creating effective resilience plans that combine risk- and capability-based strategies is critical to managing the full range of potential disruptions (Herbane, 2010a; Gibb & Buchanan, 2006). Different methodological approaches to risk management and business continuity reflect different philosophical underpinnings, since while risk management is commonly conducted with a quantitative examination and probabilistic modeling to evaluate and prioritize threats, business continuity provides a scenario-based planning and capability development to anticipate the variety of potential hazards (Elliott & Swartz, 2010; Herbane, 2010a). Contemporary scholarship shows that both strategies are essential for a holistic system of organizational resilience: quantitative risk analysis for an organized approach to known threats, and scenario-based continuity planning to address both unexplored and emergent challenges (McManus et al., 2008; Burnard & Bhamra, 2011).

As organizations recognize the need for coordinated approaches to maximize the correlation between prevention and survival capabilities (Gibb & Buchanan, 2006; Sahebjamnia et al., 2015), integration strategies for risk management and business continuity have become increasingly important. Current frameworks have focused on creating integrated governance

structures, shared information systems, and coordinated investment strategies to align businesses' risk management and business continuity efforts, ensuring they are aligned and mutually reinforcing (Elliott & Swartz, 2010; Business Continuity Institute, 2024). The development of unified resilience management frameworks has become important for ensuring that risk management and business continuity investments are optimized and coordinated (Sahebjamnia et al., 2015; Bhamra et al., 2011).

Through the information-sharing and coordination mechanisms of risk management and business continuity functions, organizations can use threat intelligence and vulnerability assessments for continuity planning, while employing continuity exercises and incident experience to strengthen their risk assessment and mitigation strategies (Business Continuity Institute, 2024; Elliott & Swartz, 2010). Contemporary approaches to integration emphasize the importance of developing shared data platforms, common terminology and frameworks, and regular communication and collaboration processes to facilitate effective coordination (Sahebjamnia et al., 2018). The development of integrated risk and continuity management systems has become important for enabling real-time information sharing and coordinated decision-making (Bhamra et al., 2011; Burnard & Bhamra, 2011). More recent studies reveal that such organizations, which integrate risk management and business continuity functions, generally require different organizational configurations, procedures, and skills or competencies from those that separate these tasks (Sahebjamnia et al., 2018; Elliott & Swartz, 2010). The development of integrated competency frameworks and training programs has become important for supporting workforce development and organizational capability building (Business Continuity Institute, 2024; Elliott & Swartz, 2010).

Performance measurement and evaluation considerations for integrated risk management and business continuity require comprehensive approaches that assess both prevention effectiveness and survival capabilities (Elliott & Swartz, 2010; Herbane, 2010a). Contemporary frameworks are focused on developing balanced scorecards and KPIs that capture the value of both risk reduction and continuity capabilities (Business Continuity Institute, 2024; ISO, 2019). The development of integrated performance measurement systems has become important for demonstrating the combined value of risk management and business continuity investments to stakeholders (Gordon & Loeb, 2002; Business Continuity Institute, 2024).

Technology integration considerations for risk management and business continuity require platforms and solutions that support both threat monitoring and operational continuity

objectives (NIST, 2024; Business Continuity Institute, 2024). Recent technology integration trends emphasize building architecture for the risk intelligence and continuity elements, such as threat detection and preventive safety protection for the risk and recovery systems, ensuring that the system (such as a backup infrastructure) can help mitigate both damage and recovery operations (NIST, 2024; Sahebjamnia et al., 2018). Integrated technology platforms are important in achieving investment efficiency and operational effectiveness (Business Continuity Institute, 2024; ISO, 2022b).

3.3. Standards and frameworks

Standards and frameworks in business continuity management and their application are critical enablers of organizational resilience, providing structured approaches and standard terminology, and offering best-practice recommendations that enhance the efficiency and reliability of continuity planning and implementation (Business Continuity Institute, 2024; ISO, 2019). Recent work indicates that standards-based business continuity can serve as an effective enabler of organizational capability by establishing methods, tracking and comparing activities, and facilitating collaboration and alignment across organizations and sectors (Business Continuity Institute, 2024; Zsidisin et al., 2005). The emergence of business continuity standards attests to the discipline's maturity and the growing acceptance of continuity as a vital organizational capability requiring systematic and professional management (FINMA, 2024).

ISO 22301, Business Continuity Management Systems, is a leading international standard for business continuity management, providing detailed requirements for establishing, implementing, maintaining, and continually improving such systems (ISO, 2019). This standard is based on a process-based approach that integrates business continuity with organizational strategy and risk management, requiring organizations to conduct business impact analysis, risk assessment, and continuity strategy development as foundation elements (ISO, 2019).

The ISO 22301 framework provides a Plan-Do-Check-Act cycle to facilitate the continuous improvement of business continuity capabilities through systematic planning, implementation, monitoring, and review (ISO, 2019). The standard mandates that organizations establish continuity objectives and policies that align with organizational strategy; develop and implement continuity plans and procedures to address identified risks and impacts; monitor and measure continuity performance through exercises and assessments; and review and improve continuity capabilities using lessons learned and evolving circumstances (ISO, 2019).

The development of comprehensive continuity measurement frameworks requires new approaches, including the Business Continuity Institute's influential framework, which provides detailed guidance on BCP and implementation across multiple organizational contexts and industry sectors (Business Continuity Institute, 2024). The guidelines emphasize a lifecycle approach to business continuity that encompasses understanding the organization, determining the business continuity strategy, developing and implementing the business continuity response, exercising and maintaining it, and embedding business continuity in the organizational culture (Business Continuity Institute, 2024). Recent research shows that Business Continuity Institute recommendations provide practical guidance that aligns with organizational demands and circumstances (Business Continuity Institute, 2024).

The NIST's Special Publication 800-34, Contingency Planning Guide, provides an extensive overview of business continuity in information technology settings and emphasizes the importance of integrating business continuity into cybersecurity and information security plans (NIST, 2010). The guide provides a seven-step process for developing a contingency plan and the planning itself that includes constructing a contingency planning policy, conducting a business impact analysis, identifying preventive controls, creating contingency strategies, developing information system contingency plans, ensuring plan testing and exercises, and maintaining the plans (NIST, 2010). NIST theory promotes risk-based planning and integrates business continuity into broader organizational risk management frameworks (NIST, 2024; Bhamra et al., 2011). Sectoral frameworks have been developed to address the needs and constraints of sectors such as financial services, healthcare, telecommunications, and critical infrastructure (Salvi et al., 2022; Assenza et al., 2024). Regional and national frameworks provide regulatory alignment across diverse regulatory landscapes and cultural contexts, while remaining consistent with best practices (European Commission, 2023; Fahey, 2024). The European Committee for Standardization developed CEN/TS 17091, 'Crisis management – Guidance for developing a strategic capability', offering European guidance on crisis management approaches; it has since been superseded by EN ISO 22361:2022 (ISO, 2022c). The framework guides the development of strategic crisis management capability within organizations (CEN, 2018).

Recent paradigms explore emerging challenges and opportunities in business continuity management, including digitalization, decentralized organizations, supply chain resiliency, and climate change adaptation (Business Continuity Institute, 2024; Rapaccini et al., 2020). Cloud-native business continuity frameworks are a recent case in point, particularly as cloud

computing and workplace arrangements are shifting toward distributed work models (Rehan, 2023). In view of this, artificial intelligence and machine learning applications are reimagining business continuity, leading to the emergence of new frameworks that employ sophisticated analytical tools for risk assessment, impact prediction, and response optimization (Sarker, 2022; Prakash et al., 2024). When introducing standards and structures for business continuity management principles or frameworks, key factors such as organizational context, resource constraints, and stakeholder demands should be considered (Business Continuity Institute, 2024; ISO, 2019).

Contemporary research suggests that successful implementation must be grounded in strong leadership commitment, appropriate resources, comprehensive training and awareness programs, and sustained efforts (Herbane, 2010a; Gibb & Buchanan, 2006). The development of implementation roadmaps and maturity models has become important for guiding organizations through the complex process of building business continuity capabilities (Brezavšček & Baggia, 2025; Business Continuity Institute, 2024).

Certification and assessment schemes enable organizations to demonstrate adherence to business continuity standards and benchmark their capabilities against best-in-class industry practices (ISO, 2019; Business Continuity Institute, 2024). Organizations may seek independent third-party certification of their business continuity management system against ISO 22301 (ISO, 2019). Professional certification programs such as the Business Continuity Institute's certification schemes provide individual practitioners with recognized credentials and continuing education opportunities (Business Continuity Institute, 2024).

Challenges in implementation

The implementation of business continuity management is hindered by complex, multidimensional challenges that can have substantial implications for organizational efforts to establish and sustain effective continuity capacity (Herbane, 2010a; Gibb & Buchanan, 2006). Research documents a collection of different types of challenges that organizations must address in order to implement business continuity successfully: resource constraints that make investing in continuity capabilities infeasible; resistance and cultural barriers by organizations that restrict the adoption of continuity initiatives; difficulty in planning and implementation related to complexity and coordination; problems measuring and verifying the efficacy of continuity (Elliott & Swartz, 2010; Herbane, 2010a). Understanding these challenges is critical for meaningful contribution to company and stakeholder sustainability (McManus et al., 2008;

Burnard & Bhamra, 2011). Balancing continuity investments with other business priorities while operating within financial and personnel resource constraints creates fundamental barriers to implementing business continuity (Gibb & Buchanan, 2006; Lindström et al., 2010). Contemporary studies show that business continuity requires a sustained commitment to planned analysis activities, including technology infrastructure and training, as well as to research, testing, and maintenance efforts, resulting in significant financial costs (Herbane, 2010a; Gibb & Buchanan, 2006). Without clear cost-benefit assessment metrics, the benefits of this effort may be difficult to substantiate (Gordon & Loeb, 2002; Business Continuity Institute, 2024). Business case studies are one way to gain better insight into economics and benefits of ongoing continuity capacity (Gordon & Loeb, 2002).

Challenges in organizational culture and change management stem from the need to shift organizational culture, behavior, and attitudes toward a continuity orientation (Business Continuity Institute, 2024; Elliott & Swartz, 2010). Modern evidence shows that organizational continuity necessitates cultural adjustments from a reactive to a proactive paradigm, from personal to common responsibility, and from short-term to long-term thinking, all of which clash with current organizational values and culture (Alshaikh, 2020; Elliott & Swartz, 2010). Organizational continuity requires the persistence of leadership endorsement, ongoing change initiatives, and the recurrent application of culture-building across systems, processes, and practices (Bhamra et al., 2011; Burnard & Bhamra, 2011). Complexity and coordination challenges are symptomatic of the complexity of contemporary organizations and the need to coordinate continuity activities among different functions, locations, and stakeholder communities (Linkov & Kott, 2018; Dupont, 2019). Recent work shows that business continuity cannot be achieved through intervention strategies but only through holistic strategies that also account for the interplay among people, processes, technology, and other organizations (Bhamra et al., 2011; Burnard & Bhamra, 2011). Organizational interdependencies, management, and coordination of continuity initiatives across heterogeneous stakeholder groups are challenging problems that call for enhanced governance and communication (Elliott & Swartz, 2010; Gibb & Buchanan, 2006). Skills and competency issues encompass the need for specialized knowledge and abilities that may not be available in current organizational workforces ((ISC)², 2023; Business Continuity Institute, 2024).

Recent literature suggests that business continuity requires interdisciplinary skills, including risk management, operations management, project management, and crisis management, which complicate the management of qualified personnel recruitment, training, and retention

(Business Continuity Institute, 2024; Elliott & Swartz, 2010). There is a recognized need for new business continuity competency frameworks and training programs that address continuity and incorporate diverse disciplinary perspectives (Business Continuity Institute, 2024; (ISC)², 2023). Challenges in technology integration and legacy systems arise because systems must maintain continuity across a variety of, often aging, technological environments (Wallace & Webber, 2017; Snedaker, 2013). Current reports indicate that organizations face ongoing challenges integrating new continuity technologies with legacy systems that may be inflexible and unable to effectively support continuity (Wallace & Webber, 2017; Snedaker, 2013). The growth of migration strategies and hybrid solutions that combine traditional and new technologies is crucial for facilitating continuous transformation, preventing disruption to critical business operations, and connecting legacy and new systems (Business Continuity Institute, 2024; ISO, 2022b). Testing and validation pose challenges for evaluating continuity capabilities without incurring real-world disruptions (European Commission, 2023; European Parliament and Council of the European Union, 2022a). Recent literature suggests that standard testing methods are insufficient to ensure the ability to manage business continuity, as tests conducted under stress, uncertainty, and surprise are often unfeasible to replicate in a controlled setting (Elliott & Swartz, 2010; McManus et al., 2008).

Given the nature of such risks, it is essential to develop creative solutions that model high-complexity, dynamic-disruption scenarios and provide valuable insights into continuity capabilities to inform the development of realistic testing and exercise programs (FINMA, 2024). The regulatory environment for business continuity is evolving and may lack clear guidelines for its implementation, leading to uncertainty and potential compliance risks for organizations (European Commission, 2023; European Parliament and Council of the European Union, 2022a). Compliance-specific continuity strategies must therefore be implemented without conflict, with a focus on understanding the regulatory context and engaging with regulators (Herbane, 2010a; Gibb & Buchanan, 2006). Issues with supply chain and third-party coordination are primarily attributable to the need to build continuity capabilities between suppliers, partners, and service providers (Sheffi, 2005; Christopher & Peck, 2004). In recent years, it has been demonstrated that business continuity success depends on communication and coordination among business actors with diverse goals, capacities, and circumstances (McManus et al., 2008; Christopher & Peck, 2004). Realizing multi-organizational continuity frameworks requires rethinking how we collaborate and coordinate, and how to address diverse

interests and achieve common continuity objectives (Gibb & Buchanan, 2006; Lindström et al., 2010).

Challenges in measuring and evaluating performance hamper the implementation of business continuity, and it is also difficult to determine whether investment in continuity is useful and demonstrates value to stakeholders (Business Continuity Institute, 2024; ISO, 2019). Recent literature claims that performance measures framed within established standards are inadequate for assessing business continuity or the capacity to handle uncertainty and surprise, which are difficult to capture (McManus et al., 2008; Elliott & Swartz, 2010). There is a need to develop holistic approaches that integrate quantitative performance indicators with qualitative capabilities for adaptation and learning, thereby creating comprehensive frameworks for measuring continuity (Business Continuity Institute, 2024; Elliott & Swartz, 2010). These sustainability and maintenance problems highlight the crucial need for durability and continuity amid protracted change, enabling organizations to address evolving internal dynamics and threat environments (Sahebjamnia et al., 2018). Previous studies have shown that many business continuity programs lose efficacy over time due to insufficient attention or resource shortages/prioritized efforts (Bhamra et al., 2011; Burnard & Bhamra, 2011). Since the advent of sustainable continuity models that can address evolving circumstances while retaining core capabilities (Linkov & Kott, 2018; Dupont, 2019), these have become essential for longer-term success.

Future developments

Over the coming decades, the evolution of business continuity will be shaped by multiple converging trends that will fundamentally transform how organizations plan for, implement, and manage continuity across industries (Malatji et al., 2022; Sepúlveda Estay et al., 2020). Several converging trends are likely to shape the future of business continuity, including AI and machine learning, cloud-native and distributed architectures, ecosystem-wide continuity capabilities, and evolving regulatory and governance frameworks (Business Continuity Institute, 2024; Elliott & Swartz, 2010). A clear understanding of these trends is critical for organizations seeking to develop forward-looking continuity strategies that can adapt to technological evolution, the business environment, and government regulations (Ivanov, 2020; Queiroz et al., 2022). The development and application of artificial intelligence and machine learning are significant trends in business continuity and may enable organizations to manage risk better, predict outcomes, and respond effectively (Ivanov, 2020; Queiroz et al., 2022).

Recent studies have demonstrated the capabilities of artificial intelligence-enabled continuity solutions in predictive threat detection, automated impact assessments, intelligent resource allocation, and adaptive response optimization to enhance operational continuity (Sarker, 2022; Prakash et al., 2024). An emerging frontier in which artificial intelligence-based continuity platforms that learn from experience and adapt to new situations may change the nature of business continuity management (Prakash et al., 2024). Cloud computing and distributed architectures can support continuity, but they also introduce security risks and provider dependencies that must be managed (Subashini & Kavitha, 2011; Business Continuity Institute, 2024). Modern studies show that cloud-native continuity architectures can provide features such as real-time backup and recovery, automatic geo-distribution, and elastic resource allocation, thereby substantially reducing the complexity and cost of continuity implementation (Business Continuity Institute, 2024; ISO, 2022b). Remote work and digital collaboration technologies are also important trends that will affect how organizations maintain continuity capabilities (Lallie et al., 2021).

The COVID-19 pandemic, according to recent research, has further accelerated the adoption of remote work and online collaboration, potentially providing organizations with flexibility and resilience while posing new threats to security, coordination, and cultural management (Lallie et al., 2021; Papadopoulos et al., 2022; Seetharaman, 2020). Sustainability and climate change adaptation are emerging considerations that organizations must integrate into their continuity capabilities to address long-term environmental impacts and evolving regulatory requirements (Business Continuity Institute, 2024). In accordance with recent research, climate change is causing more frequent and severe natural disasters, while creating new types of risks, including the disruptions of supply chains, changes in regulations, and the expectations of stakeholders, which must be met via increasing business continuity capabilities (Sahebjamnia et al., 2015; Business Continuity Institute, 2024). These new approaches to sustainability, including continuity, business continuity, change, and risk management, would be key, as they would drive changes in priorities and investment decisions across organizations (Sheffi, 2005; Christopher & Peck, 2004). Ecosystem and supply chain resilience have emerged as a fundamental trend, acknowledging the interdependence of contemporary business operations and requiring coordinated capabilities to ensure continuity across organizations and sectors (McManus et al., 2008; Burnard & Bhamra, 2011). Industry-wide and cross-sector continuity initiatives are significant trends that have the potential to greatly strengthen collective resilience capabilities (Ponomarov & Holcomb, 2009; Christopher & Peck, 2004; FFIEC, 2019).

Regulatory evolution and harmonization are important trends that will affect how organizations approach BCP and implementation (European Commission, 2023; European Parliament and Council of the European Union, 2022a). Modern research indicates that the regulatory environment for business continuity is evolving rapidly and becoming more exhaustive and prescriptive, resulting in new requirements and opportunities (Business Continuity Institute, 2024; Elliott & Swartz, 2010). The emergence of international industry standards and frameworks for business continuity is also a relevant trend, as it creates new opportunities for international collaboration and reduces regulatory compliance burdens (Business Continuity Institute, 2024; ISO, 2022b). Combining cybersecurity and digital resilience represents a contemporary development in understanding business continuity and cybersecurity as complementary and interrelated fields (Bhamra et al., 2011; Burnard & Bhamra, 2011).

The latest studies show that cyber threats are evolving; they are not only more sophisticated and persistent but also more demanding of a continuum function than simply operating interruption, which focuses on incidents in cyberspace (Linkov & Kott, 2018; Dupont, 2019). Developing integrated cyber-physical continuity frameworks is an important trend that may help address hybrid threats to system resilience (Malatji et al., 2022; Sepúlveda Estay et al., 2020). The measurement and analytics transformations are significant trends expected to enable organizations to assess their capacity for continuity, conduct rigorous assessments, and refine their performance (Li, 2018; Sarker, 2022). More recent research also shows that data analytics, simulation, and modeling tools are enabling new types of continuity measurement (Ivanov, 2020; Queiroz et al., 2022). Systems for real-time continuity monitoring and optimization are developing capabilities that could significantly enhance and maintain continuity (Ivanov, 2020; Queiroz et al., 2022).

Stakeholders are asking organizations to provide information on their continuity capabilities and demonstrate operational resilience (Business Continuity Institute, 2024; Elliott & Swartz, 2010). Stakeholder-focused continuity reporting and communication frameworks have emerged as an important trend that could change the organizational focus and practice (Elliott & Swartz, 2010; CISA, 2023a). Personalization and customization are emerging trends that recognize that continuity solutions must accommodate diverse organizational contexts, industry needs, and stakeholders' expectations (Business Continuity Institute, 2024; ISO, 2022b). Recent literature also indicates that an absolute one-size-fits-all approach to business continuity is often ineffective, and that systems' development and adaptation capabilities must be sophisticated (European Commission, 2023; European Parliament and Council of the European Union,

2022a). Modular and configurable continuity frameworks are a growing trend aimed at the smooth and efficient fulfillment of continuity requirements (Federal Council, 2023; FINMA, 2024).

3.4. Business continuity planning and its determinants

Proper implementation of BCP initiatives depends on several interrelated determinants that can foster effective organizational preparedness and response capabilities, but these initiatives must be carefully managed and coordinated (Business Continuity Institute, 2024; Elliott & Swartz, 2010). The Business Continuity Institute has identified several critical determinants of BCP success: leadership commitment and governance; organizational culture and change management; resource allocation and investment strategy; stakeholder engagement and communication; and continuous improvement and learning (Business Continuity Institute, 2024; Elliott & Swartz, 2010). Leaders' support for and endorsement by executives have been recognized as major factors indicating BCP success, as organizational commitment, resource allocation, and cultural acceptance are influenced by sponsorship from leaders who encourage at the organizational level (Herbane, 2010a; Davison, 2008). The adoption of BCP practices requires an organizational culture that prioritizes employee participation. Organizations that foster collaboration and learning are more likely to achieve successful outcomes than those with rigid, hierarchical cultures (Herbane, 2010a; Elliott & Swartz, 2010). Adequate resource distribution and clear investment strategies are fundamental determinants of a BCP's scope and quality. This requires sustained investment in planning, technology, and training (Business Continuity Institute, 2024). Establishing investment strategies that optimally allocate limited resources to support strategic planning is critical to its success (Business Continuity Institute, 2024; ISO, 2022b). BCP requires cross-functional coordination and integration across operations, human resources, and finance (Sahebjamnia et al., 2018).

An effective BCP requires organized engagement with customers, suppliers, regulators, investors, and other stakeholders to address their expectations and requirements (Business Continuity Institute, 2024; Elliott & Swartz, 2010). Thus, there is an emergent need to address these issues through effective stakeholder-oriented planning that accommodates and addresses the various, and sometimes conflicting, requirements (Herbane, 2010a; Gibb & Buchanan, 2006). Capabilities in risk assessment and business impact analysis are fundamental technical determinants that shape the quality and effectiveness of BCP outcomes (Sheffi, 2005; Christopher & Peck, 2004). More recent research shows that organizations with a more

advanced approach to risk assessment and impact analysis will develop a better, more targeted business continuity plan than firms lacking such capability (McManus et al., 2008; Burnard & Bhamra, 2011). Advanced analytical methods that target both quantitative and qualitative components of risk and impact assessment have emerged as critical to successful planning (Gibb & Buchanan, 2006; Lindström et al., 2010). The integration of technology infrastructure and systems is important for determining how effectively BCP leverages digital technologies to enhance preparedness and response capabilities (Gibb & Buchanan, 2006; Elliott & Swartz, 2010). Recent studies indicate that organizations with a strong, well-integrated technology infrastructure achieve better BCP outcomes than those with fragmented or legacy technology contexts (Craighead et al., 2007; Peck, 2005). Technology-driven planning strategies, including cloud computing, mobile technologies, and artificial intelligence, appear to be popular trends for incorporating advanced planning capabilities (Business Continuity Institute, 2024; Elliott & Swartz, 2010).

Testing and validation capabilities help assess the extent to which plans and procedures remain effective during BCP disruptions (Sahebjamnia et al., 2018). However, modern research demonstrates that businesses with extensive testing and exercise programs are more likely to implement effective BCP than companies with minimal or no testing programs or that rarely conduct testing (Bhamra et al., 2011; Burnard & Bhamra, 2011). Both the technical and organizational scope of continuity plans should be assessed in test programs that require practical testing (McManus et al., 2008; Business Continuity Institute, 2024). A process that is continually improved through lessons learned from training and other applied events is essential to maintaining the BCP's sustainability, dynamism, and effectiveness over time (Herbane, 2010a; Lindström et al., 2010).

Leadership is a critical component of BCP, extending beyond executive sponsorship to encompass strategic vision, cultural change, and resource provision. BCP is often framed by strong leadership and requires effective leadership to ensure that it is not merely a technical exercise but a key ingredient of organizational purpose and sustainable commitment (Herbane, 2010a; Business Continuity Institute, 2024). In addition, embedded in the top-down business organization strategy, BCP should also contribute critically to resilience. This alignment ensures that continuity capabilities align with strategic objectives and can be a source of competitive advantage (Herbane, 2010a; Sahebjamnia et al., 2018).

Challenges in planning

The implementation of BCP faces challenges, including resource constraints, organizational complexity, and difficulties in measuring effectiveness (Elliott & Swartz, 2010; Herbane, 2010a). The challenges of resource allocation and investment are the bedrock barriers to business continuity planning, as organizations must balance planning investments against other business priorities and are constrained by financial and human resources (Gibb & Buchanan, 2006; Lindström et al., 2010). BCP is a long-term effort involving investment in analysis and planning, technology infrastructure, training, testing, and maintenance; these investments can be difficult to justify without clear evaluation of their organizational value (Gibb & Buchanan, 2006; Elliott & Swartz, 2010; Business Continuity Institute, 2024).

3.5. The importance of business continuity planning

Protection of organizational assets through BCP is considered a strategic imperative, encompassing physical infrastructure, intellectual property, personnel, capital, and reputation (Sahebjamnia et al., 2015). There is a notable difference in asset protection among organizations with comprehensive BCPs: organizations that followed BCPs were observed to have substantially greater protection than those with ad hoc planning, particularly during operational disruptions, as conventional risk management was unable to control them (Elliott & Swartz, 2010). As organizational systems have become more complex and interdependent, new vulnerabilities have emerged, thereby increasing the strategic importance of BCP (Herbane, 2010a; Peck, 2005). Fundamentally, physical asset protection continues to cover facilities, equipment, and infrastructure, while the protection of information and intellectual property has become paramount as organizations get increasingly reliant on knowledge-based assets and digital systems (McManus et al., 2008; Craighead et al., 2007).

Regulatory frameworks across jurisdictions strengthen the obligations to protect assets. The NIST has produced comprehensive guidance that integrates physical, cyber, and business continuity risk models (NIST, 2024; CISA, 2023a). The EU has taken holistic steps through the Critical Infrastructure Protection Directive and the Network and Information Security Directive, while the DORA establishes comprehensive obligations for the financial sector (European Commission, 2023; European Parliament and Council of the European Union, 2022a). It is not limited to a financial framework such as that in Switzerland, which has established an elaborate, regulated approach through the Financial Market Supervisory

Authority, emphasizing risk-driven planning, ongoing assessment and monitoring, and the incorporation of corporate governance (FINMA, 2024).

There is a different importance to protecting reputational and supply chain assets from a supply chain security perspective, because these can be permanently affected if the market becomes vulnerable; even a small loss is permanent (Sahebjamnia et al., 2015; Gibb & Buchanan, 2006). Operational continuity is a core goal of BCP and addresses how to maintain essential functions during service continuity to minimize service interruptions (Craighead et al., 2007). Organizations with strong operational continuity capabilities perform markedly better in such scenarios, as they can mitigate downtime and enhance stakeholder satisfaction (Business Continuity Institute, 2024; Elliott & Swartz, 2010). Recent empirical findings further demonstrate that organizations with mature business continuity management practices achieve significantly higher levels of operational resilience and performance during disruptions (Yulianto et al., 2025). Through business impact analysis, organizations identify critical functions and prioritize them to allocate resources to critical processes (Wallace & Webber, 2017; Snedaker, 2013). The ability to implement alternative operating procedures and technology redundancy (e.g., cloud computing and distributed architectures) is critical, enabling organizations to maintain the capacity to sustain mission-critical functions and activities when normal conditions are disrupted (Ivanov, 2020; Business Continuity Institute, 2024).

Human resource continuity, supply chain diversification, and communication continuity are other important aspects; the organization's operational impact on other actors will always be significant because operational processes are affected by disruptions in these dimensions, even in the absence of internal capabilities (FINMA, 2024). The continuity of customer service and product and service quality in the face of disruptions is imperative to ensure relationship retention and regulatory standing (Gibb & Buchanan, 2006; Business Continuity Institute, 2024).

Revenue protection, insurance optimization, and cash flow management (Sheffi, 2005) are significant financial levers that affect BCP. Cash-flow disruptions may trigger secondary financial crises that are more severe than the initial disruption, necessitating liquidity management (Burnard & Bhamra, 2011). Disruptive cost containment, uninterrupted financial reporting, and optimization of recovery costs are additional facets that enable organizations to remain compliant with regulations and reassure stakeholders during adverse periods (Malatji et

al., 2022; Ivanov, 2020). Long-term financial impact management is highly important, as disruptions may lead to a protracted competitive disadvantage and low profitability lasting for months or years (Business Continuity Institute, 2024).

Improving stakeholder confidence

BCP is a key strategic advantage that enhances stakeholder confidence, extending beyond immediate crisis management to include building long-term relationships and value (Federal Council, 2023; FINMA, 2024). Customer confidence is directly associated with revenue and competitive advantage; organizations with strong continuity capabilities experience lower customer churn and greater satisfaction (Herbane, 2010a; Gibb & Buchanan, 2006). Supplier and partner trust, employee security, and regulatory trust are additional aspects that effective BCPs strengthen, thereby enhancing organizational relationships and reputation (Craighead et al., 2007; Linkov & Kott, 2018). The framework of relationships comprises community trust, media relations, and international credibility; organizational models that exhibit a thorough continuity process enjoy broad market coverage and a stronger general social license (McManus et al., 2008). BCP is increasingly concerned with regulatory compliance, as national governments worldwide have adopted laws mandating business continuity (Gibb & Buchanan, 2006). The European Union has established elaborate frameworks, for example, through the Network and Information Security Directive (NIS2) and the DORA, which detail the business continuity planning, testing, and reporting requirements of all EU financial institutions (European Commission, 2023; European Parliament and Council of the European Union, 2022a).

With respect to financial regulations, FINMA Circular 2023/1 establishes risk-based requirements for operational risk and resilience in Swiss banks (FINMA, 2022). These frameworks are supplemented with sector-specific regulations in telecommunications, energy, and healthcare (Federal Council, 2023). Regulatory coordination worldwide, through the Basel Committee on Banking Supervision and the International Organization of Securities Commissions, continues to drive the trend toward harmonized operational resilience standards across jurisdictions (FINMA, 2022; Dupont, 2019).

BCP can provide a significant competitive advantage by enabling firms to continue serving customers when competitors cease operations (Malatji et al., 2022). Business continuity can create competitive advantages by enabling continued service during disruption and strengthening supply-chain relationships (Sheffi, 2005; Christopher & Peck, 2004).

Importantly, BCP processes spur innovation via organizational learning and agility, whilst revealing operational efficiencies that generate enduring cost benefits (Herbane, 2010a; Gibb & Buchanan, 2006). The competitive position of well-prepared organizations is further strengthened by risk management benefits, including reduced insurance costs and improved talent retention (Business Continuity Institute, 2024; Linkov & Kott, 2018). Long-term organizational viability is an important objective of BCP because continuity capabilities help organizations sustain critical operations during disruption (Business Continuity Institute, 2024; Elliott & Swartz, 2010). Ivanov (2020) demonstrates how simulation can help organizations anticipate supply-chain disruption impacts and evaluate mitigation strategies. As the frequency and intensity of climate-related events (e.g., natural disasters) increase, environmental sustainability and climate resilience have become determinative dimensions of risk management (Business Continuity Institute, 2024). The dimensions of economic sustainability, technological resilience, and governance sustainability further help ensure that organizations remain viable across financial, technological, and institutional dimensions (FINMA, 2024; Gibb & Buchanan, 2006). The long-run stability of a business can rely on continuity strategies that emphasize innovation, because a company capable of preserving innovative competence amid disruption would possess a sustainable competitive advantage (Sahebjamnia et al., 2018; Business Continuity Institute, 2024).

3.6. Definition of the specifics of cybersecurity resilience in business

The identification and analysis of industry-specific cyber resilience requirements is a core prerequisite for constructing successful organizational defense strategies, as each sector presents its own set of threats, regulations, operational risks, and vulnerabilities, which require organizations to approach cyber resilience implementation with some level of customization (Panteli et al., 2025; Razzaq & Shah, 2025).

The Swiss financial market oversight authority has developed a comprehensive banking cyber-resilience standard that sets out requirements for managing operational risks, including cyber resilience (FINMA, 2024). Sector-specific cyber resilience in Switzerland emphasizes voluntary collaboration, industry best practices, and the flexibility to impose mandatory requirements when necessary (Federal Council, 2023; FINMA, 2024). Telecommunications organizations require a specific cyber-resilient capability to protect network infrastructure and telecommunications services that are essential to supporting other critical sectors on which telecommunications companies depend (Porambage & Liyanage, 2023; Aldea et al., 2023).

Modern studies indicate that, in telecommunications, cyber resilience for such organizations needs to be tailored to the sector's specific needs. It should be a multifaceted challenge encompassing network security, customer information protection, and service continuity in the event of a cyber incident (Porambage & Liyanage, 2023; Aldea et al., 2023). The telecommunications industry's cyber resilience agenda has been further complicated by the advent of 5G networks and the growing convergence of telecommunications and information technology infrastructure systems (Porambage & Liyanage, 2023; Aldea et al., 2023). Government cyber-resilience requires coordination among public authorities and cooperation with private-sector and academic actors (Federal Council, 2023).

Role of technology in resilience

Technology underpins cyber resilience by providing vulnerability information and enabling defensive and recovery capabilities that allow a company to continue operations during an attack and recover without disruption (Conklin et al., 2017; Linkov & Kott, 2018). Modern research shows that companies with advanced technology configurations and security technologies perform far better than low-technology organizations in contemporary cyber-resilience outcomes, compared with their older systems and limited technology capabilities (Järveläinen et al., 2025). The cyber resilience-tech dimension of cyber is much more complex, as the rise of cloud computing, AI, the device-based Internet of Things, and other innovations represents new opportunities for improved resilience and increased susceptibility (Järveläinen et al., 2025).

Artificial intelligence and machine learning solutions are crucial enablers of modern cyber resilience capabilities, enabling enterprises to detect, analyze, and respond to cyber threats at scale and speed, which would be impractical with standard methods (Sarker, 2022; Prakash et al., 2024). Recent research also shows that artificial intelligence security technologies significantly increase threat-detection accuracy and reduce false-positive rates and facilitate automated responses that enhance overall resilience (Sarker, 2022; Prakash et al., 2024). In contrast, the development of AI tools also introduces new threats and attack surfaces that organizations must mitigate through comprehensive AI security strategies (Sarker, 2022; Barredo Arrieta et al., 2020). Cloud technologies enhance organizations' cyber resilience through backup and recovery, geographic availability, and advanced security services (Subashini & Kavitha, 2011; Rehan, 2023). As established in recent studies, organizations can expect shorter recovery times and less downtime during disasters by leveraging well-designed

cloud-based architectures to enhance on-site resilience to cyber events, rather than relying on legacy infrastructure (Subashini & Kavitha, 2011; Rehan, 2023). However, cloud adoption has introduced new dependencies and a shared-responsibility model, necessitating management approaches to ensure resilience (Subashini & Kavitha, 2011; Rehan, 2023).

Zero-trust architecture is an emerging approach to cyber resilience (technological) that relies on no implicit trust and requires verification of every access request, regardless of location/user credentials (NIST, 2020; CISA, 2023b). Recent research demonstrates that implementing zero-trust mechanisms can enhance cyber resilience by reducing malicious activity and restricting lateral movement across networks (NIST, 2020; CISA, 2023b). Zero-trust implementation requires integrating technologies and exercising judiciously to realize the expected resilience benefits (NIST, 2020; CISA, 2023b). Security orchestration, automation, and response technology helps entities enhance cyber resilience through automated threat detection, analysis, and response that run at machine speed (Ahmad et al., 2020; Razzaq & Shah, 2025). Recent studies have shown that implementing security orchestration, automation, and response measures can significantly reduce incident response times and improve the consistency of response actions (Razzaq & Shah, 2025). Automation technologies, however, require careful design and testing to avoid introducing new vulnerabilities and interfering with the activities of legitimate enterprises (Barredo Arrieta et al., 2020; Prakash et al., 2024). Backup and disaster recovery technologies are fundamental components of cyber resilience, enabling organizations to restore operations and data following a cyber incident (Snedaker, 2013; Wallace & Webber, 2017). Modern studies show that organizations with well-constructed backup strategies and proven recovery protocols typically have much shorter recovery times than those with limited backup environments (Snedaker, 2013; Wallace & Webber, 2017). The most advanced backup solutions include cloud-based backup, immutable storage, and air-gapped systems, which increase security and prevent attacks such as ransomware (Snedaker, 2013; Wallace & Webber, 2017).

Network segmentation and micro-segmentation technologies enable organizations to mitigate the impact of successful cyberattacks by confining threats to specific network segments (NIST, 2020). As a result, modern research shows that a successful network segmentation not only minimizes lateral movement but also restricts access to critical systems (NIST, 2020; CISA, 2023b). Innovative segmentation techniques, such as software-defined networking and network access control, provide dynamic, adaptive segmentation capabilities (NIST, 2020; CISA, 2023b). Identity and access management technologies are critical to cyber resilience as they

prevent unauthorized access to organizational systems and data (NIST, 2020; CISA, 2023b). Identity and access management measures are intended to reduce unauthorized access and limit an attacker's ability to move laterally through organizational systems (NIST, 2020; CISA, 2023b). Advances in identity and access management, such as multi-factor authentication, privileged access management, and identity governance, enhance security and resilience (NIST, 2020; CISA, 2023b). Encryption is a crucial protective technology for organizational information and communications, enabling information protection when systems are at risk (Nadji, 2024; Razzaq & Shah, 2025). Recent studies indicate that complex encryption operations can mitigate information loss and extend recovery time (Nadji, 2024; Razzaq & Shah, 2025). FIPS 203 specifies a key-encapsulation mechanism believed to be secure even against adversaries possessing a quantum computer (Alagic et al., 2024). Security information and event management technologies allow organizations to aggregate, analyze, and respond to security events throughout their technology infrastructure (Aldea et al., 2023; Muhati & Rawat, 2024). Modern studies demonstrate that successful Security Information and Event Management implementation can significantly enhance threat detection and accelerate incident response (Aldea et al., 2023; Muhati & Rawat, 2024). Today, modern Security Information and Event Management capabilities, such as user and entity behavior analytics and threat intelligence integration, enhance detection and analysis (Aldea et al., 2023; Muhati & Rawat, 2024).

Human factors in resilience

Human factors provide the most important, yet perhaps most susceptible, part of organizational cyber resilience, with staff, contractors, and other individuals often being the most powerful defense against cyber threats and most vulnerable target depending on their knowledge, conduct, and support from the organization (Pollini et al., 2022; Jalali et al., 2019). Recent studies show that organizations that have implemented comprehensive, human-centered cyber-resilience programs often achieve significantly better security outcomes than those that focus solely on technology solutions. Most successful cyber-attacks have been attributed to human factors (Pollini et al., 2022). As cyber attackers increasingly take their attack vectors into the human dimension, using social engineering or human manipulation techniques that circumvent even the most complex technological defenses (Nurse et al., 2011; Lallie et al., 2021), they have become increasingly important in shaping cyber resilience. On the other hand, cybersecurity awareness and education are key elements of human-centered cyber resilience, as they enable employees to identify and respond appropriately to cyber threats (Alshaikh, 2020).

Well-designed cybersecurity training can improve employees' ability to recognize and respond to phishing and social-engineering attempts (Chowdhury et al., 2022; Hatzivasilis et al., 2020). Despite the implementation of awareness programs, their effectiveness can be achieved only through consistent reinforcement, practical training, and measurement of behavior change (Chaudhary et al., 2022; Dash & Ansari, 2022). Culture and leadership support are vital drivers of the positive effects of human-centered cyber resilience programs (Da Veiga & Martins, 2015; Alshaikh, 2020). Recent studies have also demonstrated that firms with strong security cultures and visible leadership commitment are more likely to achieve higher levels of staff engagement and compliance with security policies and procedures across the organization (Flores & Ekstedt, 2016; Sonnenschein et al., 2017). Creating security-sensitive organizational cultures is a continuous process that must be embedded in broader organizational values and practices (Trim & Upton, 2013; Da Veiga & Martins, 2015). Incident response and crisis management tools rely largely on people, including training, communication, decision-making, and coordination among response team members (Ahmad et al., 2020; Thompson, 2018). Recent studies have shown that well-skilled incident response teams and effective communication protocols lead to rapid containment and recovery from cyber incidents in most organizations (Ahmad et al., 2020; Thompson, 2018). Nevertheless, stress, fatigue, and other human factors that affect incident response can significantly diminish it and should be addressed through adequate training and support (Pollini et al., 2022; Jalali et al., 2019). Risk perception and decision-making are human factors crucial to organizational cyber resilience, as they influence resource allocation, policy compliance, and strategic planning (Jalali et al., 2019; Kahneman, 2011).

Current studies have shown that cognitive biases, risk tolerance, and organizational pressures, which may play a major role in cyber risk decision-making, can affect resilience (Jalali et al., 2019; Kahneman & Tversky, 1979). These human factors must be understood and addressed in nuanced ways that account for individual and organizational psychology (Pollini et al., 2022; Jalali et al., 2019). Insider threat management is one of the most challenging human factors in cyber resilience, as trusted employees and contractors may be placed at substantial risk due to malicious actions, negligence, or compromise by others (Moustafa et al., 2021; Li et al., 2019). While some classic information security techniques can address insider threats effectively, recent research has shown that these techniques pose serious challenges—such as protecting employee privacy and trust—and compete with sophisticated solutions in terms of potential benefits (Moustafa et al., 2021; Li et al., 2019). The success of human-centred security programmes depends on understanding user behaviour, awareness, and compliance with

security policies (Moustafa et al., 2021; Li et al., 2019). Change management and adaptation are human factors that affect an organization's capacity to implement and adopt cyber resilience capabilities over time (Hiatt, 2011; Rogers, 2003). Contemporary studies indicate that strong management ability among firms is associated with greater adoption of new security technologies and processes (Hiatt, 2011; Rogers, 2003). Change management in the cybersecurity sector considers the various forms of resistance, fear, and other affective mechanisms that can impede adoption (Hiatt, 2011; Rogers, 2003). In cyber incidents, communication and information sharing are important human factors that must be ensured to ensure proper coordination and response (He et al., 2017; Fransen et al., 2015). Recent research indicates that, without the coordination and decision-making aspects of communication, cyber incidents can have significant impacts (Ahmad et al., 2020; He et al., 2017).

Technical and non-technical audiences, as well as stress- and crisis-related factors, are relevant to effective communication on cyber resilience (Ahmad et al., 2020; He et al., 2017). Training and skill development are ongoing human factors needs that should be updated to address emerging risks and technologies (Hatzivasilis et al., 2020; Chowdhury et al., 2022). Research suggests that organizational resilience is severely compromised when cybersecurity competencies are lacking, thereby impeding the implementation and maintenance of effective security measures (Hatzivasilis et al., 2020; Chowdhury et al., 2022). Filling skill gaps requires rigorous training activities that accommodate differences in learning styles, experience levels, and job functions (Hatzivasilis et al., 2020; Chowdhury et al., 2022). Psychological and behavioral factors, such as stress, fatigue, and cognitive load, strongly affect human performance during cyber incidents and routine tasks (Pollini et al., 2022; Jalali et al., 2019). Recent research has shown that under high stress, decision-making may be compromised, and the probability of error increases, thereby affecting cyber resilience (Pollini et al., 2022; Kahneman, 2011). Handling such elements entails consideration of workload, support, and organizational processes that strengthen resilience (Pollini et al., 2022; Jalali et al., 2019).

Financial aspects of resilience

Financial considerations of cyber resilience encompass the costs of implementing and maintaining resilience capabilities, as well as the economic benefits (reducing exposure to cyber risks and improving incident response) (Gordon & Loeb, 2002; Romanosky, 2016). Financial contributions are not necessarily immediately observable, but longer-term measurement methods are nevertheless required (Gordon et al., 2016). The financial aspects of cyber

resilience are attracting greater attention because cybersecurity investments must be evaluated alongside the real, quantifiable business value that companies can realize from their resilience initiatives (Gordon & Loeb, 2002; Gordon et al., 2016). Cost-benefit analysis is a key component of financial assessment in cyber resilience planning and is a tool that firms must use to evaluate the costs of resilience investments against the potential financial impact of cyber incidents (Gordon & Loeb, 2002; Gordon et al., 2016). Recent research suggests that historical cost-benefit analysis methods for assessing cyber resilience may be inadequate, as they fail to quantify risks and rewards (Gordon & Loeb, 2002; Gordon et al., 2016). Advanced financial modeling techniques, such as real options analysis and scenario-based design and forecasting, offer more effective approaches to assessing cyber-resilience investments (Gordon & Loeb, 2002; Kosub, 2015). Cyber insurance is regarded as an important tool for managing cyber risk and enhancing business resilience by providing financial coverage for losses that may not be averted through operational mechanisms (Marotta & McShane, 2018; Mukhopadhyay et al., 2019). Recent studies have revealed that the cyber insurance marketplace has undergone substantial change over the past decade, with insurers requiring more sophisticated risk management and offering a broader range of coverage (Marotta & McShane, 2018; Mukhopadhyay et al., 2019). Nonetheless, cyber insurance cannot substitute for effective cyber resilience measures and may also lead to moral hazard if organizations reduce security investments following insurance coverage (Marotta & McShane, 2018; Mukhopadhyay et al., 2019).

One of the key financial challenges of deploying cyber resilience, from the perspective of budget allocation and resource optimization, is balancing priorities amid trade-offs among competing investments (Radziwill & Benton, 2017; Kosub, 2015). The literature on modern organizations shows that effective cyber-resilience budgeting yields better outcomes than ad hoc or reactive spending (Radziwill & Benton, 2017; Kosub, 2015). To allocate the budget effectively, risks, priorities, technology dependencies, and organizational capacity must be understood (Radziwill & Benton, 2017; Kosub, 2015). Cybersecurity investment decisions should consider the expected losses associated with incidents, the vulnerability of relevant information assets, and the marginal benefit of additional controls. Incident-cost evidence can support this analysis, but it does not provide a complete lifecycle cost model for cybersecurity technologies (Gordon & Loeb, 2002; Gordon et al., 2016; Romanosky, 2016). Measuring the financial impact is essential for demonstrating the benefits of investment in cyber resilience and

for supporting further funding through resilience programs (Gordon et al., 2016; Pendleton et al., 2016).

Several studies show that organizations with more complex measurement strategies typically receive greater support for cybersecurity investments and allocate resources more effectively (Gordon et al., 2016; Pendleton et al., 2016). On the one hand, the financial impact of cyber resilience is often difficult to measure because it is difficult to quantify the number of incidents prevented and the indirect effects (Gordon et al., 2016; Pendleton et al., 2016). Thus, mechanisms (e.g., risk transfer and risk sharing) provide organizations with additional financial tools for managing cyber risk (Marotta & McShane, 2018; Mukhopadhyay et al., 2019). The existing literature suggests that efficient risk transfer is associated with substantially lower financial exposure for an organization, while leaving the required incentive for risk management behind (Marotta & McShane, 2018; Mukhopadhyay et al., 2019). Risk transfer mechanisms, however, need to be carefully designed to avoid creating coverage gaps or reducing organizational resilience (Marotta & McShane, 2018; Mukhopadhyay et al., 2019). For an economic impact analysis, organizations should consider not only direct financial losses from cyber incidents but also indirect impacts (e.g., reputational damage, customer churn, and regulatory violations) (Kosub, 2015; Tan et al., 2025). Romanosky's (2016) cost estimates capture only first- and third-party losses and exclude lost revenue, sales, and market valuation, so reported figures understate the full economic impact of large-scale cyber incidents (Romanosky, 2016), underscoring the need for a comprehensive impact assessment to inform resilience planning. Advanced economic modeling approaches enable businesses to anticipate a range of potential financial impacts (Gordon & Loeb, 2002; Gordon et al., 2016).

Investment prioritization and portfolio management techniques enable organizations to optimize their cyber-resilience investments across competing priorities and timeframes (Radziwill & Benton, 2017; Kosub, 2015). Organizations that have systematic policy investment prioritization processes are more effective at reducing risk per dollar spent on investment than their ad hoc counterparts (Radziwill & Benton, 2017; Kosub, 2015). The integration of risk assessment, business impact analysis, and financial analysis in investment prioritization is needed (Radziwill & Benton, 2017; Kosub, 2015).

Measuring resilience effectiveness

Measurement of cyber resilience effectiveness is one of the most intricate aspects of resilience management and, therefore, should also account for organizational needs and development of

comprehensive metrics and assessment approaches that can capture both quantitative performance indicators and qualitative resilience capabilities (Pendleton et al., 2016; Chaudhary et al., 2022). Current research shows that organizations with advanced programs for measuring resilience tend to deliver better resilience outcomes than organizations with less developed or ad hoc measurement approaches; nonetheless, designing effective measures relies on consideration of the context of any organization, the needs of relevant stakeholders, and the limitations of measurement (Pendleton et al., 2016; Chaudhary et al., 2022).

In an era of increasing pressure from regulators, investors, and other stakeholders to demonstrate the impact of their investments and the effectiveness of their resilience capabilities, evaluating their effects is increasingly relevant (Burch et al., 2024; Tan et al., 2025). As noted earlier, critical performance indicators for cyber resilience should encompass prevention, detection, response, and recovery capabilities, as well as technical and organizational factors (NIST, 2024; Brezavšček & Baggia, 2025). Achieving these resilient KPIs requires balancing leading indicators, which predict future performance, with lagging indicators, which measure past performance (NIST, 2024; Brezavšček & Baggia, 2025). Common resilience KPIs include mean time to detection, mean time to containment, mean time to recovery, and the percentage of critical systems with backup capabilities (NIST, 2024; Brezavšček & Baggia, 2025). Structured maturity assessment frameworks provide organizations with tools to evaluate their existing resilience capabilities and identify opportunities for improvement (Brezavšček & Baggia, 2025; Mettler, 2011).

The current studies provide evidence that maturity-driven assessment models offer substantial insight into the advantages and disadvantages of organizational resilience, thereby informing strategic planning and resource allocation (Brezavšček & Baggia, 2025; Mettler, 2011). Nevertheless, maturity evaluations should be appropriately tailored to the organization's circumstances and updated periodically to account for emerging threats and technologies (Brezavšček & Baggia, 2025; Rabii et al., 2020). Scenario-based testing and simulation provide organizations with a concrete approach to assessing resilience against real-world scenarios (Yamin & Katt, 2022; Hatzivasilis et al., 2020). Research indicates that organizations with comprehensive testing programs generally perform better in incident response than those with little or no testing (Yamin & Katt, 2022; Hatzivasilis et al., 2020). Realistic scenarios, explicit success criteria, and systematic analysis of results are key components of any effective testing program (Yamin & Katt, 2022; Hatzivasilis et al., 2020). Benchmarking and comparisons enable organizations to assess performance across industries and to identify best practices for

resilience (Pendleton et al., 2016; Chaudhary et al., 2022). Recent research indicates that benchmarking can provide useful information on relative performance and potential strengths and weaknesses (Federal Emergency Management Agency, 2018; U.S. Department of Homeland Security, 2024). However, benchmarking entails careful consideration of data quality, comparability, and confidentiality (Federal Financial Institutions Examination Council (FFIEC), 2017; NIST, 2024). Real-time assessment capabilities and ongoing monitoring enable organizations to remain well-informed about their resilience posture and respond rapidly to fluctuations in risk or capability (Aldea et al., 2023; Muhati & Rawat, 2024). According to recent studies, organizations with continuous monitoring capabilities tend to detect threats more effectively but respond to incidents more quickly (Aldea et al., 2023; Muhati & Rawat, 2024). Advanced measures such as security information and event management, user and entity behavior analytics, and threat intelligence integration provide greater visibility into resilience efficiency (Aldea et al., 2023; Muhati & Rawat, 2024).

Third-party assessment and validation provide organizations with independent verification of their resilience capabilities and their compliance with all applicable standards and requirements (Federal Council, 2023; FINMA, 2024). Modern research indicates that third-party assessment can provide external perspectives on an entity and may identify blind spots that are not apparent to internal assessment (ISACA, 2022). Third-party assessments can succeed only if judicious choices of assessors are made, and specific scope and objectives are defined (ISACA, 2022). Stakeholder feedback and stakeholder perception measurement are two relevant aspects of resilience effectiveness that influence stakeholder confidence and satisfaction among customers, investors, regulators, and other stakeholders (Freeman et al., 2020; Tan et al., 2025). Recent literature indicates that stakeholders' views can have disproportionate effects on organizational reputation and access to resources (Freeman et al., 2020). Systematic collection and evaluation of feedback from a range of stakeholders is also important for successful stakeholder measurement (Freeman et al., 2020).

Challenges in implementation

Implementing cyber resilience capabilities poses numerous challenges that organizations must address through systematic planning, adequate resource allocation, and sustained management commitment (Conklin et al., 2017; Pavão et al., 2023). Current research indicates that deploying cyber resilience within an organization is particularly challenging due to competing priorities, limited resources, technical complexity, and organizational resistance to change (Conklin et al.,

2017; Pavão et al., 2023). The environment for building cyber resilience has become increasingly challenging due to a changing threat landscape, evolving regulations, and technology dependencies, which businesses must continually adapt to and improve (Conklin et al., 2017; Verma et al., 2025). Resource limitations pose a challenge for organizations that must balance cybersecurity spending with other business requirements within tight budgets (Carías et al., 2020; Herbane, 2010b).

More recent studies, however, suggest that resource limitations may significantly constrain the depth and efficiency of resilience program adoption, particularly for smaller organizations, which often lack the financial and human resources needed to implement them comprehensively (Carías et al., 2020; Herbane, 2010b). Addressing resource-demand problems requires innovative approaches, common services, outsourcing, and stepwise implementation (Carías et al., 2020; Herbane, 2010b). Technical complexity and integration challenges arise from integrating the resilient capability across various technological environments, including legacy systems, cloud services, mobile devices, and the Internet of Things (IoT) devices (Järveläinen et al., 2025; Conklin et al., 2017).

New development studies have also demonstrated that complexity may increase implementation costs and timelines and introduce new vulnerabilities and dependencies (Järveläinen et al., 2025; Conklin et al., 2017). Solutions to technical complexity should be implemented with detailed architecture planning, a standardized set of requirements, and explicit consideration of interoperability (Järveläinen et al., 2025; Conklin et al., 2017). Resistance across the organization, as well as difficulties with change management, can impede the introduction of cyber-resilient strategies by limiting employee adoption of new policies, procedures, and technologies (Hiatt, 2011; Rogers, 2003). Recent research indicates that organizational resistance can be driven by fear of change, misunderstanding, competing priorities, and ineffective promotion of the value of resilience activities (Hiatt, 2011; Rogers, 2003). It requires both rational and emotional change-management measures to overcome resistance (Hiatt, 2011; Rogers, 2003). Cyber resilience challenges are exacerbated by skills gaps and talent shortages, as organizations struggle to find and retain cybersecurity professionals with the requisite knowledge and experience to develop effective resilience programs (Hatzivasilis et al., 2020; Paulsen et al., 2012). Recent research has shown that cybersecurity skills shortages can significantly limit an organization's capacity to implement and sustain resilience capabilities ((ISC)², 2023). This includes the importance of comprehensive training systems, attractive pay, and creative talent recruitment and retention

strategies (Hatzivasilis et al., 2020; Paulsen et al., 2012). Regulatory requirements and standards are complex because they can be inconsistent across regulatory authorities and standards (Azmi et al., 2018; Humphreys, 2008). Research has shown that compliance requirements affect the implementation of resilience interventions, increasing costs and complexity during deployment (Azmi et al., 2018; Humphreys, 2008).

Compliance with these obligations can be achieved through a structured implementation process that includes requirement mapping, gap analysis of existing model content, and the implementation of the framework within integrated systems approaches (Azmi et al., 2018; Humphreys, 2008). Vendor management and third-party risk issues stem from growing reliance on external service providers and technology vendors for critical resilience capability (Assenza et al., 2024). Recent research shows that dependencies on third parties can introduce additional vulnerabilities and make it harder for organizations to manage incidents (Assenza et al., 2024). This is why strong vendor management is important: it involves close monitoring of risks through risk assessments and contract reviews, as well as ongoing tracking of third-party performance (Assenza et al., 2024). Value issues in measurement and proof arise from the difficulty of calculating and reporting the benefits of cyber-resilience investments and the return on investment for organizational leadership (Gordon et al., 2016; Pendleton et al., 2016). Recent studies have shown that the non-physical aspects of many resilience advantages can make it difficult to justify ongoing investment and support (Gordon et al., 2016; Pendleton et al., 2016). The challenges of measurement require elaborate methods to quantify benefits and communicate the value of resilience (Gordon et al., 2016; Pendleton et al., 2016).

Future directions

Emerging technologies, evolving threat landscapes, changing regulatory requirements, and new organizational models will shape the future development of cyber resilience for businesses; resilience approaches thus need to continually adapt to new environments (Verma et al., 2025). Modern studies suggest that future cyber resilience capabilities will need to address growing cyber threats and leverage technology (including AI and quantum computing), while also exploring advanced technologies (e.g., autonomous systems) that enable threats to evolve and exploit new vulnerabilities alongside opportunities (Verma et al., 2025). The new landscape of cyber resilience will also be shaped by stakeholder expectations, regulatory requirements, and business models that emphasize sustainability, transparency, and social responsibility (Verma et al., 2025; Freeman et al., 2020). More than ever, artificial intelligence and machine learning

will become fundamental to future cyber resilience, providing organizations with improved threat detection, automated response, and predictive analytics (Sarker, 2022; Prakash et al., 2024). Today, it has been noted that AI-based resilience systems will empower organizations to respond rapidly to threats at machine speed by relieving human analysts (Sarker, 2022; Prakash et al., 2024). Nonetheless, the adoption of AI technologies will introduce new vulnerabilities, including adversarial attacks, model poisoning, and algorithmic bias, necessitating robust AI security strategies (Sarker, 2022; Barredo Arrieta et al., 2020).

Quantum computing is both an emerging threat and a potential enabler of future cyber-resilience capabilities (Razzaq & Shah, 2025). Modern studies indicate that many existing encryption algorithms may be vulnerable to quantum computers, and that new security measures, such as quantum key distribution and quantum-resistant cryptography, are emerging (Razzaq & Shah, 2025). Firms will require quantum-resilience strategies to build quantum immunity and use quantum-safe algorithms in preparation for a quantum threat (Razzaq & Shah, 2025). Zero-trust architectures and identity-centric security models are becoming fundamental aspects of future cyber resilience strategies (NIST, 2020; CISA, 2023b). Recent studies suggest that zero-trust approaches enable organizations to enhance security while supporting remote work, cloud adoption, and digitalization (NIST, 2020; CISA, 2023b). Zero trust implementation, however, will require a great transformation of organizational culture, processes, and technology architectures (NIST, 2020; CISA, 2023b). Ecosystem resilience – as well as supply chain security – is emerging as an important consideration for organizations that become increasingly reliant on complex networks of suppliers, partners, and service providers (Assenza et al., 2024). In the present study, supply chain attacks and third-party compromise are considered increasing in frequency and complexity (Assenza et al., 2024). The future of resilience should consider ecosystem-wide threats, with greater cooperation among trade institutions, information sharing, and coordinated response capacity (Assenza et al., 2024).

As countries adaptively and consistently evolve and harmonize their approaches to cybersecurity regulation, the development of increasingly comprehensive future cyber resilience needs will depend heavily on regulatory evolution (European Commission, 2023; European Parliament and Council of the European Union, 2022a). Current studies suggest that future regulatory frameworks will prioritize outcome-driven criteria, ongoing monitoring, and collaborative working between countries (European Commission, 2023; Fahey, 2024). Organizations are expected to develop a framework for adaptive compliance that balances developing regulatory requirements with operational efficiency (Humphreys, 2008; Azmi et al.,

2018). Future cyber-resilience research should continue to address evolving technologies, threat environments, and organizational adaptation requirements (Verma et al., 2025).

3.7. Dimensions of assessment of organizational resilience

Assessment of organizational resilience is increasingly becoming an advanced field of study, based on several theoretical elements and practical techniques, used to assess readiness to predict, plan, respond to, and recover from crises and disruptions, as well as to maintain operations and adjust to new situations (Verma et al., 2025; Sahebjamnia et al., 2015; Burnard & Bhamra, 2011). Recent studies indicate that a holistic resilience assessment framework should encompass multiple interrelated dimensions (Sepúlveda Estay et al., 2020; Aliyu et al., 2020). Figure 2 presents the proposed Cybersecurity Risk Maturity Assessment Framework, which integrates four assessment dimensions—Technical Capabilities, Organizational Processes, Human Factors, and Strategic & Governance—that determine Organizational Resilience. The modern organizational climate is characterized by complexity, which requires frameworks to measure risk from multiple perspectives (i.e., risk profiles, regulatory needs, and operational contexts) at the same level of consistency and comparability with respect to different organizations and sectors (Sepúlveda Estay et al., 2020; Carías et al., 2020; Assenza et al., 2024). International standards and frameworks are the core of resilience assessment, developed through empirical research and practical experience across a range of industries and jurisdictions (NIST, 2024; ISO, 2022b; Humphreys, 2008). Standardized frameworks for resilience assessment have been developed by ISO, based on ISO 22301, which addresses business continuity management, and ISO 27001, which governs information security management (ISO, 2019; ISO, 2022b; Humphreys, 2008). These international guidelines highlight risk-focused strategies that require organizations to identify, assess, and manage risks, while developing capacity for response and recovery (NIST, 2024; ISO, 2022b). Multi-dimensional assessment models offer innovative methods that recognize the complexity of organizational resilience across multiple dimensions (Büyüközkan & Güler, 2025; Carías et al., 2020).

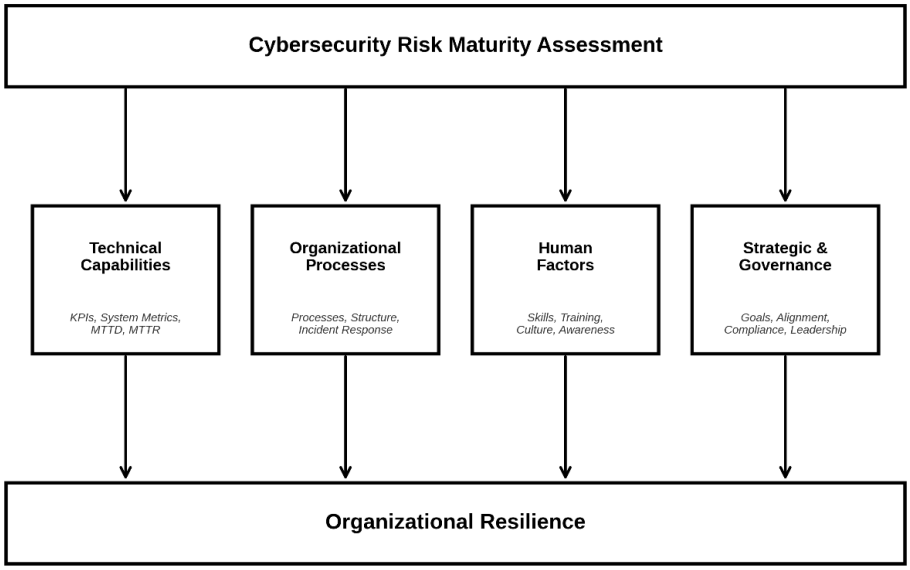


Figure 2: Cybersecurity risk maturity assessment framework

Source: Author's own elaboration, based on Bhamra et al. (2011), Linkov and Kott (2018), Malatji et al. (2022), and ISO (2022b).

Effective multidimensional models often treat technical, organizational, strategic, and human resilience as interlinked elements to be studied holistically (Verma et al., 2025; Conklin et al., 2017). Maturity-based assessment frameworks provide structured approaches for evaluating organizational resilience capabilities in terms of their sophistication and effectiveness (Rabii et al., 2020; Brezavšček & Baggia, 2025). These frameworks generally describe stages of maturity, ranging from rudimentary or ad hoc processes to more advanced capabilities (Rabii et al., 2020; Carías et al., 2020). Maturity models facilitate organizations in benchmarking their current state, identifying potential gaps, and mapping the path of resilience enhancement over time (Rabii et al., 2020; Brezavšček & Baggia, 2025; Mettler, 2011). Multiple federal agencies have developed robust assessment frameworks to evaluate resilience in the United States, showcasing best practices and national leadership in cybersecurity and the protection of critical infrastructure (CISA, 2024; NIST, 2024). The CISA has also established sectoral assessment frameworks addressing the distinct needs and risk profiles of various critical infrastructure sectors (CISA, 2024).

Table 2: Global resilience assessment frameworks and standards

Framework Category	**Examples**	**Scope & Focus**
International Governance & Management Standards	ISO 22301 (Business Continuity), ISO 27001 (Information Security), ISO 31000 (Risk Management)	Global, industry-agnostic management systems and risk protocols.
National & Strategic Security Frameworks	NIST Cybersecurity Framework (CSF) 2.0, CISA Zero Trust Maturity Model, Swiss National Cyberstrategy (NCS)	Foundational national guidelines for maturing organizational security posture.
Regulatory & Legislative Directives (Regional)	EU: NIS2, Cyber Resilience Act; Switzerland: Federal Act on Data Protection, NCSC ICT Minimum Standard	Jurisdictional laws establish mandatory minimum cybersecurity baselines.
Sector-Specific Resilience Frameworks	Finance: DORA (EU), FFIEC (US), FINMA Circular 2023/1 on Operational Resilience (CH); Critical Infrastructure: CISA Performance Goals	Industry-tailored compliance requirements and systemic risk mandates.
Technical Baselines & Assessment Methodologies	Center for Internet Security Controls / Benchmarks, FAIR-Cyber Risk Quantification	Tactical implementation metrics and financial risk quantification modeling.

Source: Author's work

The European Union has established extensive resilience assessment frameworks through the Network and Information Security Directive, the DORA, and other legislation, which emphasizes the importance of harmonized approaches among member states (European Parliament and Council of the European Union, 2022a; European Commission, 2023). The

European Union Agency for Cybersecurity (ENISA) has promoted cooperative information-sharing models, including Information Sharing and Analysis Centers, to strengthen collective resilience across sectors (European Union Agency for Network and Information Security, 2018). The EU approach focuses on risk-based assessments, helping entities align their resilience efforts with their specific risk profiles and operational environments (European Union Agency for Network and Information Security, 2018; Azmi et al., 2018). As a global financial center, Switzerland has established complex resilience assessment frameworks that indicate its commitment to maintaining high levels of robustness and reliability (Federal Council, 2023; FINMA, 2024). To achieve this, the Swiss BACS developed a range of assessments and approaches that address both public- and private-sector needs (Federal Council, 2023). The information and communication technology minimum standards published by the Federal Office for National Economic Supply also provide structured guidelines for assessing resilience in critical infrastructure (Federal Office for National Economic Supply, 2023).

Sector-specific assessment frameworks respond to sector-specific requirements and risks by addressing industry-specific expectations and unique risk profiles, while also reflecting core resilience principles and standards (Assenza et al., 2024; Salvi et al., 2022). Specialized frameworks that meet the regulatory requirements of banking supervisors and securities regulators are commonly used by financial services organizations (Assenza et al., 2024; Dupont, 2019). Healthcare companies need frameworks for patient safety, medical device security, and health information privacy (Allen, 2023). Emerging approaches to continuous assessment and monitoring acknowledge these factors as crucial and require ongoing evaluation and adaptation in light of the evolving nature of organizational resilience (Järveläinen et al., 2025; Yamin & Katt, 2022). These approaches usually integrate real-time monitoring, automated assessment tools, and continuous improvement processes (Muhati & Rawat, 2024; Aldea et al., 2023). Static monitoring methods can also be outdated, particularly in dynamic threat environments (Järveläinen et al., 2025; Muhati & Rawat, 2024).

3.7.1. Key Performance Indicators

KPIs enable organizations to track, assess, and enhance their resilience across readiness, response, recovery, and adaptation (CISA, 2024; Business Continuity Institute, 2024; ISO, 2022b). Research suggests that effective resilience KPIs, as shown in Table 3, must be identified carefully to be able to capture in detail the abilities of an organization, and to not allow for

measurement bias and gaming behaviors that can compromise assessment (European Commission, 2023; European Parliament and Council of the European Union, 2022a; Federal Council, 2023). Establishing resilience KPIs requires an understanding of organizational objectives, risk profiles, and operational settings to ensure the metrics effectively influence decision-making and improvement (FINMA, 2024). Technical performance indicators concentrate on the technology-related dimensions of organizational resilience, such as system availability, performance, security, and recovery capabilities (Pendleton et al., 2016; Yamin & Katt, 2022). An important indicator is MTTD, that is, the average time required to identify security incidents or system failures (Pendleton et al., 2016). The mean time to respond (MTTRes) reflects the average time taken to initiate response activities following incident detection (Pendleton et al., 2016). Mean time to recover (MTTRec) assesses the average time required to restore normal operations following an incident (Pendleton et al., 2016). Access and availability statistics provide simple indicators of technical resilience by quantifying the percentage of time critical systems and services remain operational and accessible (Pendleton et al., 2016). Recovery time objectives (RTOs) and recovery point objectives (RPOs) are two key indicators of acceptable downtime and data loss across business functions (Wallace & Webber, 2017).

Organizational performance indicators focus on human- and process-level aspects of resilience, such as training effectiveness, incident response coordination, communication improvement, and decision-making speed (Pollini et al., 2022; Da Veiga & Martins, 2015). Human Resource Management activities also report the extent to which employees have completed training and competency assessment scores as indicators of human capital preparedness for resilience actions (Chaudhary et al., 2022; Hatzivasilis et al., 2020).

The effectiveness and timeframe of incident response team activation and coordination measures provide insight into organizational response capabilities (Ahmad et al., 2020; Pollini et al., 2022). These metrics capture the economic aspects of resilience and assess the cost-effectiveness of resilience investments, the financial implications of incidents, and the return on investment (Gordon et al., 2016; Gordon & Loeb, 2002). In addition to the overall value of resilience capabilities, the total cost of ownership is also assessed holistically, including direct investment, recurring costs (operations), and opportunity costs (Gordon et al., 2016; Gordon & Loeb, 2002). The cost per incident and cost-avoidance measures indicate a financial benefit of resilience investments (Gordon & Loeb, 2002; Radziwill & Benton, 2017). These strategic performance indicators assess alignment of resilience capabilities with organizational

objectives, such as competitive advantage, stakeholder confidence, and long-term sustainability (European Commission, 2023; European Parliament and Council of the European Union, 2022a; Federal Council, 2023). These resilience capabilities correlate with customer satisfaction scores and retention rates (FINMA, 2022; FINMA, 2024).

Regulatory compliance scores and audit findings are methods for assessing the alignment of resilience skills with external needs (Azmi et al., 2018). Risk-based performance indicators, therefore, focus on the effectiveness of resilience capacities in managing specific risks and threats (Marotta & McShane, 2018; Pendleton et al., 2016). Security threat detection and false positive rates indicate the effectiveness of monitoring (Pendleton et al., 2016). Vulnerability assessment scores and remediation rates reflect measures of proactive risk management strategies (Pendleton et al., 2016). They also allow organizations to assess resilience competency against industry benchmarks, best practices, and regulatory expectations (Brezavšček & Baggia, 2025; Radziwill & Benton, 2017). To this end, both industry ranking scores and peer comparison metrics provide external validation of resilience capabilities (Brezavšček & Baggia, 2025; Radziwill & Benton, 2017).

Maturity assessment scores offer a systematic means of assessing development over time (Rabii et al., 2020; Brezavšček & Baggia, 2025; Mettler, 2011). Leading and lagging indicators reflect different approaches to resilience performance: leading indicators focus on proactive actions and capabilities, whereas lagging indicators center on outcomes (Linkov & Kott, 2018; Dupont, 2019). Hours of training per worker and the frequency of exercise participation are leading indicators of preparedness (Hatzivasilis et al., 2020; Chaudhary et al., 2022). Incident frequency and impact severity are lagging indicators of resilience effectiveness (Pendleton et al., 2016; Ahmad et al., 2020).

Table 3: KPIs for organizational resilience

KPI Category	Key Metrics	Measurement
Technical Performance	MTTD, MTTR, RTO, RPO, System availability, System recovery success rate	Time-based and Ratio-based
Organizational Performance	Training effectiveness, Incident response activation time,	Process-based

	Communication speed, Decision-making speed	
Human Capital Preparedness	Training completion rates, Competency assessment scores, Employee preparedness, Hours of training per worker	Capability-based
Financial Metrics	Total cost of ownership, Cost per incident, Cost avoidance measures, Return on investment	Cost-based
Compliance & Strategic Indicators	Regulatory compliance scores, Audit findings, Customer satisfaction scores, Retention rates, Industry ranking scores	Outcome-based
Risk-Based Indicators	Threat detection rates, False positive rates, Vulnerability assessment scores, Remediation rates	Rate-based

Source: Author's work

Note: MTTD = Mean Time To Detect; MTTRes = Mean Time To Respond; MTTRec = Mean Time To Recover; RTO = Recovery Time Objective; RPO = Recovery Point Objective.

3.7.2. Role of technology in assessment

Technology is a key factor in assessing organizational resilience through automated data collection, real-time monitoring, advanced analytics, and holistic reporting, thereby enhancing the accuracy and efficiency of assessment processes (Muhati & Rawat, 2024; Aldea et al., 2023). Recent studies indicate that technology-supported evaluation approaches provide more holistic and timely perspectives than traditional manual assessment systems, while reducing pressure on organizational capacity and increasing the reliability of assessment outputs (Muhati & Rawat, 2024; Moustafa et al., 2021). The application of newer technologies, such as artificial intelligence, machine learning, and big data analytics, is transforming resilience assessment practices from static, stop-start assessments to continuous, dynamic monitoring and evaluation processes (Sarker, 2022; Prakash et al., 2024).

Automated monitoring and data collection systems are fundamental technological capabilities that enable continuous assessment of resilience indicators across technical, organizational, and strategic levels (Muhati & Rawat, 2024; Moustafa et al., 2021). Security Information and Event Management systems enable comprehensive monitoring of security events and incidents, enabling analysis to assess detection, response, and recovery capabilities (Muhati & Rawat, 2024; Aldea et al., 2023). Network monitoring tools give real-time insight into system performance, availability, and security status (Muhati & Rawat, 2024; Prakash et al., 2024). Analytics and intelligence platforms have enabled complex analyses of assessment data, uncovering trends and insights that would not be detectable through either quantitative or qualitative methods (Muhati & Rawat, 2024). Machine learning techniques can be applied to analyze historical incident records to identify risk factors for potential future incidents (Barredo Arrieta et al., 2020; Prakash et al., 2024). Predictive analytics may enable organizations to anticipate resilience threats and mitigate the likelihood of vulnerability exploitation (Prakash et al., 2024). Organizations could test their resilience technologies, simulation, and modeling capabilities in a risk-free environment (Yamin & Katt, 2022; Hatzivasilis et al., 2020). The "Cyber range scenarios" offer a realistic testing ground for incident responses and recovery strategies (Yamin & Katt, 2022; Hatzivasilis et al., 2020). Tools for business continuity simulation enable organizations to simulate the effects of various disruptions and assess the performance of their plans to cope with and mitigate them (Yamin & Katt, 2022; Wallace & Webber, 2017).

Automated data collection, real-time monitoring, and anomaly visualization can improve the timeliness of technical security analysis (Aldea et al., 2023; Muhati & Rawat, 2024). These frameworks encompass questionnaire management, evidence collection, gap analysis, and reporting systems (Prakash et al., 2024). The automated scoring and benchmarking feature allow organizations to compare their performance to industry standards and peer organizations (Brezavšček & Baggia, 2025). Dashboard and visualization technologies provide user-friendly graphical interfaces for displaying assessment information, enabling stakeholders to understand resilience status and trends (or lack thereof) (Muhati & Rawat, 2024; Aldea et al., 2023). Executive dashboards provide senior administrators with corporate-level overviews of resilience performance (Muhati & Rawat, 2024; Aldea et al., 2023). Operational dashboards are designed to provide operational, technical, and managerial information to IT teams and operational managers (Muhati & Rawat, 2024; Aldea et al., 2023). Integration and interoperability capabilities allow assessment technologies to communicate and share data

across diverse systems and platforms (Muhati & Rawat, 2024; Moustafa et al., 2021). Application programming interfaces (APIs) allow various assessment tools to share data and coordinate activities (Aldea et al., 2023).

Standardized data formats and protocols make assessment results available for sharing across multi-organizational and cross-jurisdictional levels (Barredo Arrieta et al., 2020; Prakash et al., 2024). Cloud-based assessment platforms can be implemented and deployed rapidly and cost-effectively, as scalable, accessible tools available across geographic boundaries (Subashini & Kavitha, 2011; ISACA, 2022). Where assessment capabilities are delivered through cloud services, cloud-specific security risks and dependencies must be considered (Subashini & Kavitha, 2011). Additionally, cloud platforms enable collaborative assessment work among diverse stakeholders and organizations (Subashini & Kavitha, 2011; ISACA, 2022). To develop higher-order analytics and automated insights, artificial intelligence and machine learning solutions are increasingly being incorporated into assessment mechanisms (Sarker, 2022; Prakash et al., 2024). Natural language processing can analyze unstructured data, such as incident reports and policy documents (Sarker, 2022; Prakash et al., 2024). This information is useful for an assessment (Sarker, 2022; Prakash et al., 2024). Anomaly detection algorithms can identify unusual patterns in assessment data that may indicate emerging risks or vulnerabilities (Muhati & Rawat, 2024; Sarker, 2022).

3.7.3. Human factors in resilience assessment

Human factors such as knowledge, skills, attitudes, behaviour, and organizational culture influence cybersecurity outcomes (Pollini et al., 2022; Flores & Ekstedt, 2016). Human factors should be assessed across individuals, organizational behavior, and organizational processes, in the context of interactions among people, processes, and technology (Pollini et al., 2022; Flores & Ekstedt, 2016). The leadership and governance assessment explicitly examines the role of senior management and organizational leadership as stakeholders in defining the resilience vision, strategy, and culture (Sonnenschein et al., 2017; Flores & Ekstedt, 2016).

A good leadership assessment appraises the extent to which senior executives are committed to developing resilience initiatives, their awareness of the need for resilience, and their capacity to make appropriate resource-allocation decisions (Sonnenschein et al., 2017; Flores & Ekstedt, 2016; Freeman et al., 2020). Governance assessment evaluates the structures, processes, and accountability mechanisms that guide resilience activities across an organization (Sonnenschein et al., 2017; ISO, 2022b). Competency and skills assessment measures the capability of

individuals and their team members to carry out resilience activities (Pollini et al., 2022; Chaudhary et al., 2022; Hatzivasilis et al., 2020). Technical competency assessment considers the tailored knowledge required to undertake specific resilience actions, such as incident response, business continuity planning, and risk management (Chaudhary et al., 2022; Hatzivasilis et al., 2020). Soft skills assessment evaluates communication, coordination, decision-making, and problem-solving capacity, which are necessary to achieve effective resilience outcomes (Pollini et al., 2022; Jalali et al., 2019). Training and awareness assessment measures the effectiveness of educational and communication programs to build resilience capabilities across the organization (Chaudhary et al., 2022; Hatzivasilis et al., 2020). Training assessment assesses the design, delivery, and results of formal training programs (Chaudhary et al., 2022; Hatzivasilis et al., 2020).

The awareness assessment refers to the extent to which people know about and engage with their organizations' resilience policies, procedures, and expectations (Li et al., 2019; Flores & Ekstedt, 2016). Cultural and behavioral assessment includes social values and beliefs that influence how people and groups interact with resilience tasks (Da Veiga & Martins, 2015; Flores & Ekstedt, 2016). A safety culture assessment measures the organizational focus on, and the extent of, safety and risk management in decision-making and everyday life (Da Veiga & Martins, 2015; Pollini et al., 2022). Drawing on experience-based learning behavior within organizations, this assessment focuses on the learning culture that drives the organizational environment to continuously seek improvement and adapt to experience and feedback (Ahmad et al., 2020; Da Veiga & Martins, 2015). The assessment of communication and coordination assesses the effectiveness of information sharing and collaborative activities during both normal operations and crises (Pollini et al., 2022; Ahmad et al., 2020). Internal communication assessment evaluates the quality and timeliness of information sharing throughout the organization (Pollini et al., 2022; Ahmad et al., 2020). The external communication assessment measures organizations' communications with customers, partners, regulators, and other stakeholders (Freeman et al., 2020; Ahmad et al., 2020).

Assessments of decision-making and problem-solving address the cognitive and organizational processes that inform choices and actions during resilience efforts (Jalali et al., 2019; Kahneman & Tversky, 1979). The Individual Decision-Making assessment evaluates the quality of choices made by key personnel under stress and uncertainty (Kahneman & Tversky, 1979; Jalali et al., 2019). Collective decision-making assessment aims to evaluate the effectiveness of group processes in managing competing priorities in complex stakeholder-involved decision-making

(Pollini et al., 2022; Ahmad et al., 2020). Stress and performance assessment targets the effect of stress and pressure on individual and organizational performance (Pollini et al., 2022; Chowdhury et al., 2022). Stress testing assesses the performance of participants or groups in simulated crises (FINMA, 2022; Yamin & Katt, 2022). Performance degradation analysis assesses capability over time under varying levels of pressure and resources (Chowdhury et al., 2022; Pollini et al., 2022). The assessment of motivation and engagement examines the factors that motivate individuals and groups to engage in resilience (Flores & Ekstedt, 2016; Da Veiga & Martins, 2015). An intrinsic motivation assessment examines the belief that resilience work is meaningful and rewarding for individuals (Flores & Ekstedt, 2016; Da Veiga & Martins, 2015). Organizational engagement assessment is about the extent to which personal goals align with organizational resilience goals (Flores & Ekstedt, 2016; Da Veiga & Martins, 2015).

3.7.4. Best practices

The most common techniques and models for resilience assessment in organizations are best practices that stem from the development of research methods and evidence-based approaches across organizations and disciplines (Järveläinen et al., 2025; Tan et al., 2025). The determination of best practices must be based on the organizational context, resources, and sector-specific strategic objectives, and must ensure consistency with industry standards and regulatory requirements (Brezavšček & Baggia, 2025).

Comprehensive, integrated assessment methods are fundamental best practices that respect the multifaceted nature of organizational resilience (Järveläinen et al., 2025; Tan et al., 2025). Good assessments generally encompass the technical, organizational, and strategic dimensions of resilience, drawing on diverse data sources (Järveläinen et al., 2025; Brezavšček & Baggia, 2025). Integrating different assessment areas can identify potential interdependencies or shortcomings that may not have been recognized by isolated assessments (Järveläinen et al., 2025; Aldea et al., 2023). Risk-based assessment prioritization enables organizations to focus on the most salient areas and highest-priority risks (Marotta & McShane, 2018; Gordon & Loeb, 2002). Priority-based assessment allocation ensures that limited resources are directed toward the most important resilience capabilities (Gordon & Loeb, 2002; Radziwill & Benton, 2017).

Stakeholder engagement and participation are critical best practices that help ensure evaluation outputs reflect the organization's diverse viewpoints and realities (Sonnenschein et al., 2017; Freeman et al., 2020). Engagement from senior management is vital, as it provides strategic direction and sufficient resource allocation (Sonnenschein et al., 2017; Freeman et al., 2020).

Cross-functional participation facilitates the identification of interdependencies and ensures that assessment outcomes are relevant across organizational areas (Ahmad et al., 2020; Aldea et al., 2023). Ongoing and iterative evaluation methods recognize that resilience is a transient construct and, therefore, a dynamic process that requires continuous evaluation and recalibration (Järveläinen et al., 2025). Organizations that conduct regular assessment cycles are also better able to monitor progress over time to detect emerging risk or changing needs (Brezavšček & Baggia, 2025). Resilience performance can be assessed in real time through continual monitoring to adapt quickly to changes in state conditions (Muhati & Rawat, 2024; Aldea et al., 2023).

Evidence-based assessment methods rely on objective data and factual information rather than on subjective opinions or assumptions (Yamin & Katt, 2022). Review of documentation, system testing, and performance measurement serves as objective measures of resilience capabilities (Yamin & Katt, 2022; Brezavšček & Baggia, 2025). Further objective and credible verification by independent third-party assessments and peer reviews could also ensure independence and objectivity (ISO, 2022b; Brezavšček & Baggia, 2025). Actions and improvement planning ensure that assessment activities are associated with tangible gains in resilience capabilities (Brezavšček & Baggia, 2025). Assessment results should include specific recommendations for addressing the identified gaps and weaknesses (Rabii et al., 2020; Brezavšček & Baggia, 2025). Timelines, resource requirements, and accountability mechanisms need to be planned for implementation (Wallace & Webber, 2017). Organizations can use benchmarking and comparison to assess their resilience capabilities against industry norms and peer organizations (Brezavšček & Baggia, 2025). Industry benchmarking provides an overarching perspective on the assessment findings and helps identify areas for improvement (Brezavšček & Baggia, 2025). Identifying good practice allows organizations to learn from others' experiences (Brezavšček & Baggia, 2025; Rabii et al., 2020). Assessment technologies enable more intelligent assessment by leveraging tools from other contexts, helping assessors work more efficiently and effectively (Muhati & Rawat, 2024; Aldea et al., 2023). Automated data retrieval minimizes manual intervention and increases reliability (Muhati & Rawat, 2024; Brezavšček & Baggia, 2025). Analytical tools, such as visualization software, can be applied towards pattern detection and trend analysis in assessment data (Aldea et al., 2023).

Table 4: Comparative analysis of major resilience assessment frameworks

Assessment Framework	**Jurisdiction**	**Scope**	**Target Group**	**Key Components**	**Assessment Frequency**
NIST Cybersecurity Framework (CSF) 2.0	United States	Comprehensive cybersecurity and resilience across all sectors	All organizations; mandatory for US federal agencies	Govern, Identify, Protect, Detect, Respond, and Recover functions with 22 categories	Voluntary; annual for U.S. federal agencies
CISA Cyber Resilience Review	United States	Critical infrastructure resilience	Critical infrastructure operators	Ten domains, including: Asset Management, Controls Management, Incident Management, and Service Continuity Management	Voluntary; frequency not specified.
NIS2 Directive	European Union	Network and information security resilience	Essential entities across 18 sectors	Risk management, incident handling, business continuity, supply chain security	Incident reporting (24h/72h); periodic national strategy review
ENISA Handbook for Cyber Stress Tests (European Union Agency for Cybersecurity, 2025)	European Union	Systemic cyber resilience	National and sectoral authorities overseeing the critical sector	Scenario-based testing, dependency analysis, and recovery capabilities	Periodic, based on risk profile
NCSC Minimum Standard for	Switzerland	Critical ICT infrastructure resilience	Critical infrastructure operators,	Based on NIST CSF: Identify, Protect,	Self-assessment tool provided; frequency not mandated

Assessment Framework	Jurisdiction	Scope	Target Group	Key Components	Assessment Frequency
Improving ICT Resilience			financial institutions	Detect, Respond, Recover	
FINMA Circular 2023/1 Operational Risks and Resilience – Banks	Switzerland	Financial sector operational resilience	Banks, securities firms, financial groups, and conglomerates	Operational risk management, business continuity, outsourcing, cyber risk	Annual reporting, on-site examinations
ISO/IEC 27001:2022	International	Information security management systems (ISMS)	All organizations seeking certification	Clauses 4-10 (Context, Leadership, Planning, Support, Operation, Evaluation, Improvement) and 93 controls	Annual surveillance, triennial recertification

Source: Author's work

A comparison of the cyber resilience assessment measures presented in Table 4 indicates considerable differences in their scope, approaches, and requirements (NIST, 2024; FINMA, 2022; ISO, 2022b; CISA, 2020). The NIST Cybersecurity Framework (CSF 2.0) is one of the most general (and often broader) frameworks applied across industries, whereas sector-specific frameworks (e.g., FINMA Circular 2023/1) are tailored to the needs of specific industries (NIST, 2024; FINMA, 2022). The Minimum standard for enhancing ICT resilience is considered the most context-specific for Switzerland, integrating international best practices and specific considerations for preserving critical infrastructure (Federal Council, 2023). Assessment duration and resource requirements vary with scope and complexity. The CISA Cyber Resilience Review is an interview-based assessment of operational resilience and cybersecurity practices (CISA, 2020). The variances are attributable to variation in scope,

complexity, and regulatory requirements, rather than to improved effectiveness (Brezavšček & Baggia, 2025; Järveläinen et al., 2025).

This chapter has positioned cyber resilience as a core of contemporary business continuity. Instead of treating continuity solely as a responsive IT function, this study views resilience as a proactive, sociotechnical construct driven by technological infrastructure, human competence, and the maturity of adaptive governance. The discussion structure aligns the discussion around core competencies, such as incident containment, strategic flexibility, and organizational learning, with globally recognized standards like ISO 22301 and the NIST frameworks by operationalizing an organization's capability for anticipating, absorbing, and recovering from cyber incidents. In the end, framing targeted assessment dimensions in this way moves the narrative from simply synthesizing concepts to a practical means of measuring them, laying the strong methodological groundwork for the empirical analyses presented in the next chapters.

4. THE IMPACT OF CYBERSECURITY RISK MATURITY ON RESILIENCE

This chapter integrates the theoretical perspectives developed in the previous chapters to present a holistic model of how cybersecurity risk maturity influences organizational resilience. It examines aspects of cybersecurity risk maturity, including risk identification, control effectiveness, and continuous monitoring. Namely, the relationship of resilience and cybersecurity significantly increases an organization's resistance and recovery capacity against cyberattacks and other threats (Durst et al., 2024). Preventive resilience in cybersecurity refers to the actions taken to prevent cyber incidents (Salvi et al., 2022). A comprehensive strategy for increasing the protection against cyber risks requires that business models be in place across the network with a wide range of technologies, such as systems modernization, enhanced security architectures, regular updates, up-to-date patches, and system personnel training in cybersecurity (Trim & Upton, 2013; Verma et al., 2025).

Preventive resilience involves advanced threat intelligence capabilities, proactive vulnerability management programs, and a holistic security architecture that addresses emerging threats stemming from developments such as AI-facilitated attacks, quantum computing penetration, and complex supply chain compromises, all of which define today's threat landscape (Verma et al., 2025). As described by Carías et al. (2020) and Salvi et al. (2022), adaptive resilience is an organization's capacity to respond to and recover from cyberattacks. For instance, one such initiative would incorporate flexible cybersecurity technologies and be supported by a dynamic, adaptable security infrastructure, including incident response teams and disaster recovery planning (Onwubiko, 2020). Technologies for adaptive resilience are continually evolving, integrating real-time threat detection with AI and ML to automate responses to novel attack patterns and enable organizations to respond dynamically to emerging cyber threats (Razzaq & Shah, 2025). Responding to cyber threats across organizational and technological boundaries requires coordinated processes for monitoring, analysis, communication, and response (Verma et al., 2025; Ahmad et al., 2020). A rapid response to a cyberattack reduces downtime and mitigates impacts on key operations. Furthermore, the predictive aspect of the relationship entails employing predictive analytics and threat intelligence to anticipate cybersecurity threats and vulnerabilities (Razzaq & Shah, 2025).

The most recent predictive resilience framework incorporates threat intelligence from dark web monitoring, geopolitical analysis, and industry-specific threat feeds. These provide comprehensive situational awareness to mitigate risk (Saeed et al., 2023).

The concept of collaborative resilience emphasizes cooperation and information sharing among actors, including businesses, government organizations, and international partners (Verma et al., 2025). Current collaborative resilience models promote the development of cyber threat intelligence-sharing systems, industry-specific information-sharing and analysis centers (ISACs), and public-private collaborations to facilitate the real-time exchange of threat information and support coordination and response (Verma et al., 2025; He et al., 2017). Collaborative resilience can be strengthened through structured threat-information sharing, joint exercises, and coordinated cross-sector response arrangements (Fransen et al., 2015; He et al., 2017; Yamin & Katt, 2022). Integrating resources and intelligence can strengthen organizations' defenses (He et al., 2017; Fischer-Hübner et al., 2021; Verma et al., 2025). The congruence between resilience and cybersecurity, on the one hand, enables a proactive strategy for managing cyber risk rather than merely reacting. It focuses on robust defenses, recovery, and learning from cyber incidents (Büyüközkan & Güler, 2025). This broader view extends to cybersecurity resilience and to more general organizational resilience frameworks, including supply chain, operational, and strategic resilience, recognizing that cyber incidents can have cascading effects across all organizational functions and stakeholder relationships (Panteli et al., 2025; Durst et al., 2024).

4.1. Key components of cybersecurity risk maturity

Amid an ever-more complex cybersecurity landscape, risk maturity is essential for organizations to maintain an effective and resilient information security posture. According to Durst et al. (2024), cybersecurity risk maturity is a model in which a company undertakes an organized effort to identify, measure, manage, and track its cybersecurity risks in accordance with its business objectives and risk appetite. Consequently, contemporary cybersecurity risk maturity has evolved into a holistic assessment approach. It defines an organization’s capacity to discover, assess, direct, and perpetually enhance its cybersecurity risk profile through integrated processes, governance, and capability-based systems (Brezavšček & Baggia, 2025). Building on this definition, it is widely accepted that mature cybersecurity risk management must be holistic, encompassing technical, organizational, and strategic perspectives. Its successful implementation requires moving beyond mere technical security controls to

understand the complexity of the current cybersecurity environment and the strategic imperatives of enterprise risk management (Büyüközkan & Güler, 2025).

Current paradigms of cybersecurity risk maturity emphasize continuous organizational learning. Practices must evolve systematically in response to incident reports, threat intelligence updates, and industry best practices to ensure vigilant, proactive risk management (Verma et al., 2025). At the heart of achieving a high level of risk maturity in cybersecurity, there must be a culture of continuous improvement that focuses on enhancing organizations' security practice by ensuring that past knowledge from the relevant events (or security incidents) can be leveraged to provide intelligence into future security practices whilst ensuring continuous adaptability to digital threats (Kosub, 2015; Durst et al., 2024; Panteli et al., 2025). As such, advanced companies tend to use a holistic approach to identify, assess, and rank potential risks and vulnerabilities across their networks, systems, and data assets (Durst et al., 2024; Almuhammadi & Alsaleh, 2017).

Emerging risks, including AI-powered attacks, quantum computing threats, supply chain weaknesses, and cloud threats—which were not adequately addressed by traditional risk assessment frameworks—are now evaluated through sophisticated risk assessment approaches such as regular vulnerability scanning, penetration testing exercises, red teaming simulations, and scenario-based tabletop exercises (Saeed et al., 2023; Yamin & Katt, 2022). These sophisticated methods replicate real-world cyberattacks, providing insight into the organization's defensive capabilities and enabling proactive steps to address potential weaknesses and implement preventive measures to mitigate associated risks. Modern risk appetite frameworks have evolved to incorporate quantitative risk modeling, most notably the FAIR model, which provides a rigorous taxonomy for quantifying cyber risk in financial terms (Freund & Jones, 2014). This allows firms to assess the overall business and financial impact of risks, bridging specific cyber-attack vectors with operational continuity and integrating security risk management directly into broader enterprise risk processes (Büyüközkan & Güler, 2025). 21st-century risk appetite frameworks, including dynamic risk appetite frameworks, now include dynamic risk tolerance mechanisms that adjust to evolving business environments, such as changing business conditions, threat environments, and regulations, whilst maintaining alignment with organizational and stakeholder goals and expectations (Büyüközkan & Güler, 2025).

Evolution of the concept of risk maturity

This section identifies that, given the ever-changing and constantly evolving nature of security problems, as well as the complexity of modern cybersecurity risks, it is important to adopt high-level, multidimensional models in cybersecurity risk from a risk management approach rather than relying solely on low-level assessment methods (Panteli et al., 2025; Razzaq & Shah, 2025; Tan et al., 2025). The growing sophistication of cyber threats has fueled the changing landscape, the increasing digitalization of organizational operations, and rising regulatory pressures that demand demonstrable cybersecurity capabilities (Brezavšček & Baggia, 2025; Verma et al., 2025). This evolution reflects the growing recognition that maintaining robust cybersecurity hygiene requires security measures grounded in systematic, disciplined risk identification, assessment, and management—moving toward continuous improvement rather than ad hoc or reactive responses (Burch et al., 2024; Durst et al., 2024; Nurse et al., 2011).

Risk maturity derives from broader organizational maturity models introduced in the 1980s and 1990s, notably the Capability Maturity Model, initially developed for software development processes (Paulk, 2002; Sepúlveda Estay et al., 2020; Brezavšček & Baggia, 2025). While early approaches existed, the CMM provided the foundation for systematically evaluating organizational capabilities across progressive maturity levels. This framework facilitated the gradual adoption of maturity concepts for cyber risk management as the field developed toward the start of the new millennium (Büyüközkan & Güler, 2025). Such initial frameworks illustrated that organizational capabilities are traceable and can be systematically assessed and improved by progressing through defined maturity tiers (NIST, 2024; Cherdantseva & Hilton, 2013; Craigen et al., 2014). Maturity concepts were initially applied to cybersecurity risk management in the early 2000s, as organizations recognized the need for more disciplined approaches to information security risk management (Cherdantseva & Hilton, 2013; Craigen et al., 2014). The integration of risk management principles and cybersecurity maturity frameworks has emerged as a focus following incidents and broader regulatory developments (NIST, 2024; Lallie et al., 2021).

The introduction of the NIST Cybersecurity Framework (NIST CSF) in 2014 represented a landmark development in cybersecurity risk maturity, bridging theoretical risk management principles with real-world operational implications. The framework integrated established practices with emerging concerns, including supply chain security, AI-related threats, and quantum computing-related risks (NIST, 2024). This model enabled organizations to

systematically evaluate and develop cybersecurity capabilities through a set of defined implementation steps (Bhamra et al., 2011; Burnard & Bhamra, 2011). Modern understanding of cybersecurity risk maturity has been substantially shaped by increasingly complex organizational risk environments and expanded IT attack surfaces (Linkov & Kott, 2018; Dupont, 2019). Cloud-based technology, digitalization, and the ubiquitous Internet of Things have raised new cybersecurity challenges, including hybrid cloud security, edge computing, AI governance, and quantum-safe cryptography, requiring advanced maturity assessments and complex risk management strategies (Brezavšček & Baggia, 2025; Malatji et al., 2022; Sepúlveda Estay et al., 2020). Organizations recognize that traditional compliance-based approaches to cybersecurity are insufficient for managing complex risk contexts (Li, 2018; Sarker, 2022).

The development of maturity in cybersecurity risk management has also been influenced by greater recognition of the link between cybersecurity risks and organizational resilience (Ivanov, 2020; Queiroz et al., 2022). Modern frameworks recognize that cybersecurity risk management must be integrated with broader organizational risk management, business continuity planning, and strategic decision-making processes. This integration recognizes that cybersecurity risks cascade across organizational functions and stakeholder relationships, underscoring the need for integrated approaches to managing operational, financial, reputational, and strategic risks (Verma et al., 2025; Ivanov, 2020; Queiroz et al., 2022). This reflects the recognition that cybersecurity risks may cascade throughout the organization and influence stakeholder relationships (Federal Emergency Management Agency, 2018; U.S. Department of Homeland Security, 2024). The European Union’s General Data Protection Regulation (GDPR) sets high-level requirements for data protection risk management, including systematic cybersecurity risk assessment and mitigation, and the NIS2 reinforces this by establishing sector-specific cybersecurity risk management obligations that require organizations to develop mature risk management capabilities (European Commission, 2023). Specifically, the European Union's GDPR includes comprehensive requirements for data protection risk management, mandating a systematic approach to evaluating and mitigating cybersecurity risks (European Parliament and Council of the European Union, 2016). These requirements were further expanded by the introduction of the NIS2, which imposes sector-specific cybersecurity risk management obligations (European Commission, 2023).

Continuing efforts by the United States, through multiple federal programs and initiatives, to develop cybersecurity risk maturity frameworks have substantially shaped the national

cybersecurity risk maturity framework. Among the most ambitious is the Department of Defense's Cybersecurity Maturity Model Certification program, a major initiative to standardize cybersecurity risk maturity assessments for defense contractors. The Cybersecurity Maturity Model Certification also requires organizations to demonstrate maturity levels commensurate with the sensitivity of the data they handle and its strategic importance within the defense supply chain (U.S. Department of Defense, 2022). The FFIEC Cybersecurity Assessment Tool, in use until its withdrawal in August 2025, exemplified sector-specific frameworks for evaluating risk maturity (Federal Financial Institutions Examination Council, 2017). The Swiss National Cyberstrategy emphasizes risk-based cybersecurity approaches that embody international best practices while accommodating Switzerland's unique position as a global financial center. This includes sophisticated approaches to risk maturity assessment that account for complex regulatory ecosystems and high-value targets characteristic of the Swiss economy (Federal Council, 2023; Sahebjamnia et al., 2015; Elliott & Swartz, 2010). The Information and Communication Technology Minimum Standards established by the Federal Office for National Economic Supply provide a Swiss version of cybersecurity risk maturity assessment (Federal Office for National Economic Supply, 2023).

Cybersecurity risk maturity comprises several interrelated aspects that jointly determine an organization's capability to identify, assess, manage, and continuously improve its cybersecurity risk posture (Sheffi, 2005; Burnard & Bhamra, 2011). More recent studies highlight that cybersecurity risk maturity extends beyond technical controls to encompass technology, strategy, and the organization as a whole. Integrating governance structures, risk assessment methodologies, control implementation protocols, monitoring capabilities, and continuous improvement processes is necessary to develop effective methods for mitigating evolving threat landscapes (Büyüközkan & Güler, 2025). In addition, several studies highlight the need to integrate technical, organizational, and strategic dimensions, rather than relying solely on technical security controls. Modern cybersecurity requires integrated methods including governance structures, risk assessment systems, control implementation strategies, and monitoring capabilities (Büyüközkan & Güler, 2025; Gibb & Buchanan, 2006; Lindström et al., 2010). Risk governance and leadership are fundamental components of cybersecurity risk maturity, defining strategic direction, accountability structures, and resource allocation mechanisms for effective cybersecurity risk management (NIST, 2024; Brezavšček & Baggia, 2025). Mature organizations implement clear governance frameworks with defined roles and responsibilities for cybersecurity risk management at all levels. When board and senior

management are involved, it is expected that the cybersecurity risks will be thoroughly embedded into corporate strategy and integrated into enterprise risk management systems (Brezavšček & Baggia, 2025; NIST, 2024).

Mature organizations have established clear governance mechanisms that delineate roles and responsibilities for managing cybersecurity risks across all levels of the organizational hierarchy. The identification and assessment capabilities are designed to help organizations systematically identify, analyze, and prioritize all cybersecurity risks (ISO, 2022a; NIST, 2024). Tools such as threat modeling, vulnerability assessments, penetration testing, and business impact analysis are used to define mature risk identification mechanisms (ISO, 2022a; NIST, 2024). Advanced technologies focus on continuous threat detection and testing through automated scanning, AI-based analysis, and real-time integration of threat intelligence. In this way, they support a more dynamic response to evolving threat landscapes and organizational environments (Verma et al., 2025). Effective risk assessment systems offer precise risk assessment and ongoing risk management. Techniques for risk identification, such as threat modeling, vulnerability assessments, penetration testing, and business impact analysis, require ongoing risk discovery in evolving threat environments with changing organizational capabilities (Linkov & Kott, 2018; Dupont, 2019). New approaches emphasize continuous risk discovery responsive to evolving threat situations and organizational contexts (Linkov & Kott, 2018). Design and execution of controls are operational aspects that translate risk assessment findings into specific security countermeasures and defense capabilities (Büyüközkan & Güler, 2025; Verma et al., 2025).

Mature organizations focus on systematic approaches to risk appetite and cost-effective control selection, consistent with industry norms and regulatory requirements. Advanced project and change management techniques are required to plan complex security deployments across multiple technological environments (Büyüközkan & Güler, 2025). The deployment of controls requires highly sophisticated project and change management skills (Büyüközkan & Güler, 2025).

The tracking and measurement capabilities enable organizations to assess how well cybersecurity risk mitigation processes perform and to identify where improvement is warranted (NIST, 2024; Brezavšček & Baggia, 2025). Advanced monitoring systems leverage multiple data sources, including Security Information and Event Management systems, vulnerability scanners, threat intelligence feeds, and KPIs. Machine learning and artificial

intelligence techniques, along with advanced analytical capabilities, facilitate the identification of patterns in emerging threats, enabling continuous assessment of cybersecurity risk (NIST, 2024; FFIEC, 2017). Incident response and recovery capabilities provide the foundation on which an organization relies to manage cybersecurity incidents effectively, enabling a timely return to normal operations (Business Continuity Institute, 2024).

Advanced incident response efforts require implementing a comprehensive set of preparatory steps, structured response mechanisms, appropriate communication, and scheduled recovery procedures, integrated with business continuity planning, to ensure that organizations have the necessary capacity to remain operational during and after a cybersecurity incident (Brezavšček & Baggia, 2025). A mature incident response program involves comprehensive preparation, structured response protocols, effective communication, and methodical recovery procedures. Continual improvement and adaptation enable an enterprise to shape its cybersecurity risk management strategies in view of new threats, technologies, and business requirements (FINMA, 2024).

Typically, mature organizations have systemic practices for learning from incidents (e.g., threat intelligence adoption, data update processes, risk assessments, and improvements in control effectiveness). The integration of continuous improvement with strategic planning ensures cybersecurity risk management is consistent with organizational goals and can account for new challenges, including AI security threats, quantum computing risks, and legislative amendments (Verma et al., 2025). Third-party risk management is increasingly important, as it addresses cybersecurity risks associated with vendor relationships, supply chain dependencies, and ecosystem partners (Saeed et al., 2023; Panteli et al., 2025). With high maturity levels, the third-party risk management program typically has due diligence processes, contractual risk allocation with tracking capabilities, and an incident coordination policy, and the complexity of modern supply chains necessitates a sophisticated approach to vendor risk assessment, which will be needed to address the multi-tier supplier relationships, dependencies on cloud services, and vulnerabilities in software supply chains (Saeed et al., 2023). A modern, structured approach to assessing and managing third-party risks is necessary given the complexity of contemporary supply chains (Saeed et al., 2023; Panteli et al., 2025).

Maturity levels and assessment frameworks

In the modern cybersecurity risk maturity approach, maturity levels are conceptualized as a hierarchical development path from lowest to highest organization capability that can contribute to the analysis of what security risk activities organizations currently have, the identification of potential performance improvements, as well as potential strategic roadmaps to improve their capabilities (Büyüközkan & Güler, 2025). Ranging from elementary compliance checklists to more complex models for evaluating cybersecurity capabilities, these have been developed to encompass elements of governance, risk management, technology implementation, human factors, and continuous improvement processes (Brezavšček & Baggia, 2025). The initial or ad hoc level typically characterizes organizations with limited formal cybersecurity risk management processes and that rely on reactive, largely individual, competence-based approaches rather than systematic ones (Brezavšček & Baggia, 2025; Büyüközkan & Güler, 2025).

Most firms in this class lack comprehensive risk assessment capabilities, governance mechanisms, systematic methods, or effective control implementation. At low maturity levels, cybersecurity measures often arise reactively in response to immediate demands or incidents rather than through a systematic, proactive risk-management strategy (Brezavšček & Baggia, 2025; Büyüközkan & Güler, 2025). At this level, the organization generally employs limited or inconsistent security practices, lacks risk insight, and does not respond appropriately to incidents (Brezavšček & Baggia, 2025). At the developing or managed level are organizations that have initiated fundamental processes for managing cybersecurity risks and are adopting a systematic approach to implementing security controls (Büyüközkan & Güler, 2025; Brezavšček & Baggia, 2025). To this level, an organization is expected to have a formal risk assessment system, written security policies, and structured responsive capabilities. However, these elements may not be well implemented throughout the organization. Also, they may not be integrated into advanced monitoring and continuous learning systems as presented in the mature layer case study (Büyüközkan & Güler, 2025). A range of risk-specific processes have been formalized, recorded, and documented by institutions at this level (Malatji et al., 2022; Sepúlveda Estay et al., 2020). Nevertheless, such approaches are not necessarily part of the organizational framework and may lack advanced tracking and improvement capabilities (Li, 2018; Sarker, 2022). At the managed or quantitatively controlled level, companies are typically designed to be guided by systematic models of risk assessment, combined mechanisms for security control, and effective incident response capabilities, as well as an approach for

consistent execution of procedures across groups of units and the quantification, measurement, and improvement, making organizations suited for constant improvement of cybersecurity capabilities (Brezavšček & Baggia, 2025). The organizations at an advanced level can be said to possess proactive threat hunting capabilities, sophisticated threat intelligence integration processes, and systematic innovation in the area of cybersecurity practices due to the optimization of cybersecurity risk management, whereby these organizations can preempt and react to new threats on their network while being operationally efficient by making strategic investments in cybersecurity to achieve business objectives (Verma et al., 2025). Cybersecurity risk management and operations management optimization enable these organizations to identify, track, and mitigate potential threats while maintaining operational efficiency (FINMA, 2024). The NIST Cybersecurity Framework covers implementation levels from Partial (Tier 1) to Adaptive (Tier 4), including Cybersecurity Risk Management as part of the organizational risk management strategy, and the most recent update, CSF 2.0, which incorporates improved maturity assessment and progression guidance (NIST, 2024).

The European Union's approach focuses on risk-based frameworks to enable organizations to understand their security needs and develop cyber defense plans aligned with their risk landscape and operational context (European Commission, 2023; European Parliament and Council of the European Union, 2022a). NIS2 sets out cybersecurity risk management requirements and establishes maturity expectations that are implicitly applicable to various organizations. DORA also imposes maturity requirements on financial services organizations that must demonstrate advanced risk management capabilities (European Parliament and Council of the European Union, 2022a). Financial institutions have been required to meet additional maturity requirements under the DORA (European Parliament and Council of the European Union, 2022a).

The ICT Minimum Standards provide a framework for assessing cybersecurity maturity, with FINMA setting maturity requirements for financial institutions based on international mainstream best practices while also considering Swiss-specific requirements related to banking secrecy, cross-border data flows, and regulatory reporting (Federal Office for National Economic Supply, 2023; FINMA, 2024).

Importance of defining risk maturity

Defining cybersecurity risk maturity, as outlined by Mettler (2011) and Brezavšček & Baggia (2025), serves several functions: helping organizations assess their capabilities, work toward

improvement, and develop strategic roadmaps to enhance their cybersecurity posture. Today, research indicates that risk maturity is often required for benchmarking, resource allocation, regulatory compliance, and communication with key stakeholders. Given organizations' increasing complexity under regulatory scrutiny and stakeholder demands, as well as competitive pressures on their cybersecurity performance (Büyüközkan & Güler, 2025), there has been a surge in demand for an explicit definition of risk maturity. Recent research shows that clear definitions of risk maturity provide a foundation for benchmarking, resource allocation, regulatory compliance, and stakeholder communication (Brezavšček & Baggia, 2025; Büyüközkan & Güler, 2025). Defining risk maturity has become a vital task for organizations due to the increasingly regulatory environment, stakeholder expectations, and competitive challenges associated with cybersecurity performance (Alexander, 2005; Linkov & Kott, 2018). Strategic planning and resource allocation are key applications of risk maturity frameworks, enabling organizations to make informed decisions about cybersecurity investments and priorities (NIST, 2024; Büyüközkan & Güler, 2025).

Transparent maturity definitions help develop maturity models to evaluate the current state of cybersecurity capabilities (with gaps that need to be addressed). With those frameworks, companies can then focus their work plans on targeted improvement to meet a business or technology need (Brezavšček & Baggia, 2025) – including evolving threats and evolution in technology as they align with business objectives, risk, and operational capacity (Brezavšček & Baggia, 2025). This ability to measure capabilities enables organizations to formulate targeted improvement plans aligned with their risk appetite, business targets, and resources, thereby facilitating progress (Büyüközkan & Güler, 2025; Ivanov, 2020). Regulatory compliance is an important driver for adopting information and cybersecurity maturity models (Brezavšček & Baggia, 2025). In many cases, formal or explicit regulation requires organizations to demonstrate systematic cybersecurity risk management, with risk maturity definitions providing a framework for documenting and communicating their cybersecurity capabilities to regulatory bodies and enabling consistent improvement efforts (Verma et al., 2025).

Benchmarking and competitive positioning are significant tools that help organizations compare their cybersecurity capabilities with those of industry peers and best practices (CISA, 2024; Business Continuity Institute, 2024). Risk maturity constructs represent universal perspectives of risk assessment, which allow for useful comparison between entities and sectors, enabling benchmarking to uncover which aspects of their operations are behind

industry standards and to enable firms to invest best in enhancing them in a manner that can be applied to the industry-specific threat and legal requirements (Büyüközkan & Güler, 2025). Through benchmarking, organizations can identify where certain areas may lag relative to industry standards and prioritize areas for improvement (European Parliament and Council of the European Union, 2022a; Federal Council, 2023).

The processes of building stakeholder communication and trust were important applications that enabled firms to help their customers, partners, investors, and other stakeholders understand their cybersecurity capabilities (FINMA, 2024). Clear definitions of risk maturity offer a way to justify cybersecurity investments and capabilities in terms that non-technical parties can comprehend, and, in light of changes such as increased demands for transparency around cybersecurity risks and management in the face of digital transformation and rising cyber threats, this process is increasingly crucial (Büyüközkan & Güler, 2025). Its enhanced communication capabilities are increasingly critical as stakeholders require greater transparency into cybersecurity risks and risk management practices (Sahebjamnia et al., 2015). Vendor and partner assessment is the practice of evaluating the cybersecurity capabilities of organizations' suppliers, service providers, and business partners (Herbane, 2010a; Gibb & Buchanan, 2006). Risk maturity definitions are structured frameworks for performing due diligence assessments and setting up minimum cybersecurity requirements for third-party relationships, as defined as necessary to manage supply chain cybersecurity risks and ensure that third-party relationships will not breach organizational security within an increasingly interconnected business environment (Saeed et al., 2023; Panteli et al., 2025).

This assessment tool can be critical for managing overall supply chain cybersecurity risk and ensuring that third-party relationships do not compromise organizational security (Saeed et al., 2023). It follows the principles of continuous improvement and organizational learning, thereby enabling organizations to systematically enhance their cybersecurity capabilities (Gibb & Buchanan, 2006; Lindström et al., 2010). The risk maturity definition framework enables organizations to measure progress, identify areas for improvement, and evolve their cybersecurity approaches to align with emerging threats, technologies, and business requirements while meeting strategic goals and stakeholder expectations. This ability to identify opportunities for improvement enables organizations to adapt to evolving cybersecurity threats (Brezavšček & Baggia, 2025). This ability to enhance capabilities helps organizations update their cyber hygiene tactics in response to evolving threats and technologies, aligning them with different business requirements (Brezavšček & Baggia, 2025; Verma et al., 2025). Investment

rationale and return-on-investment measurement are financial tools that help organizations demonstrate the value of cybersecurity investments to senior leaders and stakeholders (Business Continuity Institute, 2024; Durst et al., 2024).

Risk maturity definitions quantify cybersecurity capabilities aligned with business needs and outcomes, a measurement capability vital for securing ongoing support for cybersecurity initiatives and for demonstrating alignment with business goals, including risk reduction, improved operational effectiveness, and comparative advantage (Verma et al., 2025). Such measurement capability is critical to ensuring ongoing support for cybersecurity initiatives and to illustrating the extent to which these programs enable organizational objectives (Bhamra et al., 2011; Burnard & Bhamra, 2011).

4.2. Comprehensive overview of global cybersecurity risk maturity assessments

NIST CSF Assessment.

The NIST Cybersecurity Framework (CSF) is one of the most widely used methodologies worldwide for assessing cyber maturity. Going forward, with the introduction of CSF 2.0 in 2024, the framework was extended to all organizations, regardless of size or sector, rather than just to critical infrastructure. It draws on Implementation Tiers (1-4) (Partial, Risk Informed, Repeatable, and Adaptive) to help organizations evaluate the rigor of their risk management. This assessment addresses six key areas: Govern, Identify, Protect, Detect, Respond, and Recover. By focusing on the "Govern" function, the NIST CSF assessment underscores that cybersecurity maturity should not be assessed in isolation but should be integrated into enterprise risk management and corporate governance processes. This framework is especially appreciated for its adaptability, enabling organizations to build "Profiles" that span the gap between their current resilience and their desired target state.

Cybersecurity Maturity Model Certification Assessment

The Cybersecurity Maturity Model Certification Assessment is a specialized cybersecurity maturity framework designed for defense contractors and organizations that manage Controlled Unclassified Information (CUI). Developed and released by the Department of Defense, this framework defines three certification levels (Level 1: Foundational, Level 2: Advanced, Level 3: Expert) and includes more than 110 security practices across 14 capability domains. It has an advanced certification approach and stringent requirements. Cybersecurity Maturity Model Certification, unlike other systems, relies on independent validation of cybersecurity

capabilities and requires triennial third-party certification rather than annual self-assessment. Because of its specific emphasis on defense supply chain security, the framework is critical for organizations seeking to retain contracts with the U.S. Department of Defense.

EU Network and Information Security Directive 2 (NIS2)

The NIS2 Assessment provides harmonized cybersecurity requirements across 18 critical sectors in the European Union. It promotes risk management, incident handling, business continuity, and supply chain security through proportionate requirements based on organizational size and criticality. Implementing NIS2 requires substantial organizational resources. It is highly flexible at both the sector-specific and national levels in terms of implementation (European Commission, 2023). The framework establishes proportionate cybersecurity requirements, including mandatory incident reporting within 24 hours (as an early-warning mechanism) and within 72 hours (for full notification) (European Parliament and Council of the European Union, 2022a). The strength of NIS2 is its harmonized approach across EU Member States: aligning them on common cybersecurity standards and establishing a common set of those standards, while recognizing that differences lie at the national level of implementation.

Digital Operational Resilience Act

The DORA framework specifically addresses digital operational resilience requirements for European Union financial entities and their information and communication technology third-party service providers (European Parliament and Council of the European Union, 2022a). In line with industry-wide regulatory requirements, this framework addresses information and communication technology risk management, incident reporting, operational resilience testing, and third-party risk management. DORA provides deep specialization in financial-sector requirements, mandating ICT risk management frameworks, digital operational resilience testing, and third-party risk oversight. The framework requires at least annual review of the ICT risk management framework and periodic supervisory reviews (European Parliament and Council of the European Union, 2022a). DORA is distinctive for linking cybersecurity services to broader operational resilience and by understanding how different types of digital risks interact in the financial services sector.

Swiss ICT Minimum Standards Assessment

According to Swiss guidelines, the Swiss ICT assessment establishes criteria for critical infrastructure operators and organizations. The framework contributes to the National Cyberstrategy (NCS) 2023–2027 (Federal Council, 2023), which the Federal Council (2023) established as a strategic mandate to support the implementation of key real-world cybersecurity strategies. The Swiss framework for ICT is well-defined and aligns with international best practices; its Excel-based assessment tool scores each measure on a five-point maturity scale (levels 0 to 4) derived from the NIST Cybersecurity Framework, supported by regular self-evaluations (Federal Office for National Economic Supply, 2023). The Swiss approach provides a model for national regimes to be both compliant and interoperable internationally.

Swiss Financial Market Supervisory Authority Operational Risk Assessment

FINMA's assessment framework imposes extensive operational and cyber risk requirements on banks, insurance companies, and other industry stakeholders. FINMA developed a framework within the broader operational risk management framework, grounded in multiple circulars that articulate risk-based supervisory expectations. The FINMA framework provides comprehensive definitions for Swiss financial needs, aligned with risk-based supervisory expectations (FINMA, 2022). The framework entails annual reports plus periodic on-site inspections (FINMA, 2022; FINMA, 2024). FINMA’s methodology is a model that integrates high-level cybersecurity governance with prudential oversight—consistent with Switzerland’s status as a leading global financial center.

ISO 27001 Certification Assessment

For organizations seeking voluntary compliance and alignment with international standards, ISO 27001 Certification is the global standard for an Information Security Management System (ISMS). It comprises 93 security controls across the organizational, people, physical, and technological domains and includes comprehensive risk management requirements. ISO 27001 offers broad scope comprehensiveness and global applicability. Rather than defining maturity levels, it operates on a conformity basis: certification is granted against the standard's requirements and maintained through annual surveillance audits and triennial recertification. ISO 27001 is a process-based, widely recognized standard relevant to organizations, helping

institutions demonstrate their cybersecurity capabilities to stakeholders while prioritizing continuous improvement.

4.3. Impacts of cybersecurity risk maturity on resilience

The impact of cybersecurity risk maturity on organizational resilience is a complex, multidimensional dynamic that fundamentally shapes an organization's capability to anticipate, withstand, respond to, and recover from cybersecurity incidents whilst preserving critical functions and evolving in response to new threat environments (Durst et al., 2024; Brezavšček & Baggia, 2025; Büyüközkan & Güler, 2025). Current studies show that entities with higher cybersecurity risk maturity exhibit significantly improved resilience across multiple dimensions: technical strength, organizational flexibility, and strategic agility (Burch et al., 2024; Durst et al., 2024; Nurse et al., 2011). This correlation is informed by the recognition that resilience is not merely an outcome of a particular control but rather a result of systematic, mature approaches to risk identification, assessment, mitigation, and continual improvement (Brezavšček & Baggia, 2025; Büyüközkan & Güler, 2025; Sarker, 2022). International regulatory regimes have now widely acknowledged the relationship between cybersecurity risk maturity and organizational resilience and include requirements that implicitly or explicitly link maturity to resilience outcomes (Sepúlveda Estay et al., 2020; Brezavšček & Baggia, 2025).

The United States Cybersecurity Framework (NIST) explicitly links implementation tiers to organizational resilience capabilities in its cybersecurity model, positing that mature risk management can support incident response and recovery (NIST, 2024; Cherdantseva & Hilton, 2013). Mature organizations can adapt their cybersecurity mechanisms to shifting risk profiles and threat intelligence throughout their development life cycle, with dynamic implementation tiers as a core aspect of adaptive tiers (Cherdantseva & Hilton, 2013; Craigen et al., 2014). Cybersecurity regulation in the European Union, based on NIS2 and DORA, is consistent with the relationship between risk management maturity and explicitly defined resilience requirements (European Commission, 2023; NIST, 2024). These frameworks require organizations to implement systematic approaches to risk assessment, incident response, and business continuity that are consistent with mature risk management practices (Linkov & Kott, 2018; Dupont, 2019). The principle of proportionality embedded in these regulations acknowledges that risk maturity levels are appropriate for specific forms of organizational life while maintaining the minimum required level of resilience (Bhamra et al., 2011; Burnard & Bhamra, 2011).

Switzerland's National Cyberstrategy (NCS) 2023-2027 clearly addresses the link between cybersecurity risk maturity and national resilience by designing structures that link organizational maturity to broader national resilience goals (Federal Council, 2023). The approach highlights mature risk management practices in vital infrastructure sectors to ensure the nation's economic and social stability (Malatji et al., 2022; Sepúlveda Estay et al., 2020). Correlations between levels of cybersecurity risk maturity and multiple resilience attributes, such as incident response effectiveness, recovery time objectives, and maintenance of business continuity, are significant in empirical studies (Brezavšček & Baggia, 2025; Büyüközkan & Güler, 2025). Mature risk management processes help organizations detect incidents more quickly, develop containment strategies, respond to disasters, and recover.

Risk maturity has a role in building resilient organizations beyond the technical aspects of capability in the risk model - the culture of an enterprise, decision making, and its approach to relationships (Brezavšček & Baggia, 2025; Büyüközkan & Güler, 2025). Mature organizations tend to develop risk-conscious cultures that enable rapid decision-making, effective communication with stakeholders, and learning from incidents (Alshaikh, 2020; Ahmad et al., 2020; Pollini et al., 2022). These cultural elements are crucial for resilience, as they indicate how effectively organizations can leverage their technical activation capacity during incidents (Durst et al., 2024). Strategic integration is another crucial dimension that relies on risk maturity and resilience, since established organizations tend to adopt an integrated approach to cybersecurity risk management, including enterprise risk management, business continuity planning, and strategic planning (Rajan et al., 2021). This alignment facilitates more productive resource planning, better alignment of cybersecurity investment objectives, and greater coordination between cybersecurity and other services within the organization (Federal Council, 2023; FINMA, 2024). Cybersecurity risk management is also strategically linked to resilience, as cyberattacks can have cascading effects on internal processes and the parties involved (Panteli et al., 2025; Durst et al., 2024).

Role of risk maturity in mitigating cyber threats

Today's threat environments are evolving rapidly, becoming increasingly technical in both the quantity and variety of threat vectors, thereby requiring mature, systematic prevention and proactive threat mitigation rather than a reactive or ad hoc approach (Sahebjamnia et al., 2015; Elliott & Swartz, 2010). Organizations with higher levels of risk maturity are better equipped to mitigate multiple facets of threat, such as proactive threat hunting, advanced threat

intelligence integration, and sophisticated incident-response procedures (Brezavšček & Baggia, 2025; Büyüközkan & Güler, 2025; NIST, 2024). Proactive threat identification and assessment capabilities, along with characteristics of mature risk management (Razzaq & Shah, 2025; Verma et al., 2025), help organizations plan for potential threats before a successful attack occurs. For these organizations, established threat modeling processes are often comprehensive and systematic (NIST, 2024; Büyüközkan & Güler, 2025) in their assessment of potential attack vectors, the likelihood, and the effects of those attack vectors, and how this could lead to mitigation efforts that are prioritized based on risk-informed decision making. These capabilities are crucial to effective threat mitigation because they enable organizations to take preventive measures and build response capacity before threats arise (NIST, 2024; Büyüközkan & Güler, 2025). Advanced threat intelligence integration is a critical capability, grounded in mature risk management processes, that significantly enhances the effectiveness of threat mitigation (Razzaq & Shah, 2025; Verma et al., 2025). Mature organizations typically demonstrate robust data-collection capabilities to gather, analyze, and operationalize threat intelligence from numerous sources, including commercial threat intelligence feeds, government advisories, industry-sharing initiatives, and internal security monitoring (Razzaq & Shah, 2025). Successful threat intelligence integration requires advanced analytical capabilities and structured systems to translate intelligence into security measures (Verma et al., 2025; Business Continuity Institute, 2024).

Mature risk management creates defense-in-depth strategies with layers of protection, which dramatically improve threat mitigation (ISO, 2022a; NIST, 2024). For example, mature organizations typically adopt end-to-end security architectures that address threats across multiple layers, including the network perimeter, endpoints, applications, data, and user behavior monitoring (NIST, 2024; Linkov & Kott, 2018). This combined defense against system-level risks is important for successful protection (Alexander, 2005; Linkov & Kott, 2018) because it ensures that the failure of any single security control does not compromise the entire security system. Organizations rely on mature risk management practices, such as continuous monitoring and detection, to quickly identify threats, thereby reducing the time from the first breach to detection (Bhamra et al., 2011). A comprehensive view of security can be supported by centralized security-event monitoring, anomaly detection, and threat-intelligence analysis (Lee, 2023; Muhati & Rawat, 2024; Saeed et al., 2023). These capabilities rely on systematic collection, analysis, and operational use of security-event and threat-intelligence data (Muhati & Rawat, 2024; Saeed et al., 2023). Incident response and containment

capabilities developed through mature risk management are, in turn, useful for organizations responsible for mitigating the impact of an attack (Queiroz et al., 2022; Federal Emergency Management Agency, 2018). Organizational incident response systems typically include preparation activities, defined response processes, communication standards, and containment strategies (ISO, 2023; NIST, 2025; Thompson, 2018).

The maturity of incident response relies on robust coordination mechanisms that enable rapid deployment of response resources and support sound decisions under pressure (FFIEC, 2017; NIST, 2024). As international threat mitigation frameworks evolved, they placed greater emphasis on risk maturity as a component of building robust threat resilience (CISA, 2024; Business Continuity Institute, 2024). The United States CISA has produced wide-ranging guidance that links risk maturity across domains to specific threat-mitigation capabilities (CISA, 2024). Switzerland's approach to threat mitigation, implemented by the BACS, posits that organizational risk maturity is significantly associated with national capabilities in threat mitigation (Federal Council, 2023). Overall, national threat mitigation strategies should account for the organization's varying maturity and develop national resilience (Sahebjamnia et al., 2015).

Impact on operational continuity

The influence of cybersecurity risk maturity on operational continuity is a critical dimension through which mature risk management processes help organizations preserve critical functionality during and after cybersecurity incidents (Herbane, 2010a; Gibb & Buchanan, 2006). Operational continuity encompasses the ability to sustain critical business operations, service provision, and stakeholder relationships in the event of a cybersecurity incident (Sheffi, 2005; Christopher & Peck, 2004). For organizational effectiveness, organizations with higher cybersecurity risk maturity levels are better able to demonstrate operational continuity through more consistent business impact analysis, robust continuity planning, and the adoption of crisis management processes (McManus et al., 2008; Burnard & Bhamra, 2011). The business impact analysis capabilities supported by well-developed risk management systems enable organizations to identify core business processes accurately, determine dependencies on IT systems, and systematically prioritize continuity efforts based on their business significance (Gibb & Buchanan, 2006; Lindström et al., 2010). In mature organizations, the effects of a cybersecurity incident, both direct and indirect, can be accounted for through thorough business impact assessments (Ponomarov & Holcomb, 2009; Christopher & Peck, 2004). The basis for

this work lies in analyses that inform the development of targeted continuity strategies that allocate resources to the business functions with the highest priority (Craighead et al., 2007; Peck, 2005).

Continuity planning and preparedness activities characteristic of mature risk management provide structured options for sustaining operations during cybersecurity incidents (Business Continuity Institute, 2024; Elliott & Swartz, 2010). Effective continuity planning incorporates alternative operating arrangements, backup systems and data, alternative lines of communication, and pre-established resources capable of sustaining operations in the event of a system breakdown (Sahebjamnia et al., 2018). The continuity process should be tested, updated, and regularly trained to ensure the plan remains current and practical (Bhamra et al., 2011; Burnard & Bhamra, 2011). Mature risk management strengthens crisis management and decision-making capabilities within the organization, enabling effective responses to cybersecurity incidents (Linkov & Kott, 2018; Dupont, 2019).

Advanced crisis management often involves established governance structures, decision-makers, and authority-based authorities, procedures for maintaining effective communication, and mechanisms for systematic coordination (Malatji et al., 2022; Sepúlveda Estay et al., 2020). These capabilities enable rapid resource mobilization and informed decision-making under high-pressure conditions, ensuring the continuity of critical operations (Li, 2018; Sarker, 2022). Mature risk management, with a focus on technology resilience and redundancy strategies, constitutes the technical foundation for operational continuity (Ivanov, 2020; Queiroz et al., 2022).

The standard for information security management systems (ISMS), ISO/IEC 27001:2022, emphasizes that process maturity and continuous improvement are critical for managing security risks (ISO, 2022b). These technical capabilities enable continuous operation in the event of system failures or compromises and provide platforms for recovery activities (Federal Emergency Management Agency, 2018; U.S. Department of Homeland Security, 2024). Supply chain continuity management is an increasingly important component of operational continuity and requires advanced risk management techniques (FFIEC, 2017; NIST, 2024). In a typical mature organization, comprehensive supplier risk assessment, sourcing from alternative suppliers, and supply chain oversight skills support operations, even when suppliers are damaged or broken (NIST, 2024; CISA, 2024). The intricacies of contemporary supply chains

necessitate advanced continuity management strategies to cover direct and indirect dependencies (Business Continuity Institute, 2024; ISO, 2022b).

Operational continuity has become progressively recognized as a cornerstone of cybersecurity risk management in international regulatory frameworks (European Commission, 2023; European Parliament and Council of the European Union, 2022a). The European Union's DORA establishes operational continuity requirements explicitly tied to the maturity of risk management capabilities (European Parliament and Council of the European Union, 2022a). Analogously, the United States FFIEC has developed operational continuity requirements grounded in mature risk management practices (FFIEC, 2019). In accordance with mature risk management practices, organizations must demonstrate systematic approaches to business impact analysis, continuity planning, and crisis management, as defined by the standards (Sahebjamnia et al., 2015; Elliott & Swartz, 2010). For this reason, companies should select measurement schemes that align with regulatory compliance requirements, business needs, and the organizational environment, and that fully capture the technical, organizational, and strategic dimensions (Federal Council, 2023; FINMA, 2024).

Relationship with stakeholder confidence

The link between cybersecurity risk maturity and stakeholder confidence forms an important dimension through which evolved risk management processes impact an organization's reputation, market position, and stakeholder relationships (Sheffi, 2005; Burnard & Bhamra, 2011). In this study, stakeholder confidence refers to stakeholders' trust in an organization's ability to manage cyber risks and sustain the critical capabilities and services on which they depend (Al-Sartawi, 2020; National Institute of Standards and Technology, 2024). Organizations that have achieved maturity in their cybersecurity risk practices often generate sufficient stakeholder confidence through transparent risk communication, demonstrated security capabilities, and effective incident management (Gibb & Buchanan, 2006; Christopher & Peck, 2004). Customer and supply-chain trust can be affected by the quality of cybersecurity governance and risk management (Tan et al., 2025). Most mature companies have relatively strong customer data protection, service reliability, and incident reporting, which help customers perceive strong security capabilities (Craighead et al., 2007; Snedaker, 2013). Recently consumer awareness of cybersecurity risk has brought security capabilities to the forefront of purchasing behavior and supplier selection (Wallace & Webber, 2017; Business Continuity Institute, 2024). Investor confidence and market valuation are important

determinants of investor-stakeholder relationships and are particularly affected by expertise in cybersecurity risk management (ISO, 2022a).

Recent evidence indicates that stronger cybersecurity governance can contribute to corporate market value through investor-trust and supply-chain-trust mechanisms (Tan et al., 2025). The SEC Cybersecurity Disclosure Rules further underscore the importance of cybersecurity governance and disclosure in investor relations (Securities and Exchange Commission, 2023). Regulatory confidence, regulations, and compliance relationships are stakeholder dimensions that demand maturity in risk management (Bhamra et al., 2011). Regulatory requirements can motivate organizations to adopt and formalize cybersecurity maturity practices (Brezavšček & Baggia, 2025). The growing complexity of cybersecurity governance calls for mature risk management frameworks to demonstrate conformance and retain regulatory confidence (Büyüközkan & Güler, 2025; Brezavšček & Baggia, 2025). Partner and supplier confidence can be shaped by the quality of cybersecurity governance and supply-chain risk management (Tan et al., 2025; NIST, 2024).

Mature organizations tend to demonstrate stronger third-party risk management, supply chain security, and partnership governance, which give partners greater confidence in their security capabilities (NIST, 2024; Tan et al., 2025). In addition, public companies must establish and assess internal controls over financial reporting (U.S. Congress, 2002b). Mature risk management capability is essential, particularly within the interconnected contemporary business ecosystem, to sustain healthy partnership relationships (FFIEC, 2017; NIST, 2024).

Crisis communication and reputation management maturity in risk management enable companies to maintain stakeholder trust during cybersecurity incidents (CISA, 2024; Business Continuity Institute, 2024). Mature organizations commonly use a multifaceted communication plan to ensure that stakeholders have timely, accurate, and transparent information during a crisis (ISO, 2022c; European Commission, 2023). These communication skills are necessary to ensure that stakeholders remain confident, as they signal the organization's commitment to keeping stakeholders safe (European Parliament and Council of the European Union, 2022a; Federal Council, 2023).

Stakeholder confidence in cybersecurity risk management has been increasingly recognized through international frameworks (FINMA, 2024). Similarly, the Cybersecurity Disclosure rules issued by the United States Securities and Exchange Commission require public companies to disclose material cybersecurity incidents and information concerning

cybersecurity risk management, strategy, and governance (Securities and Exchange Commission, 2023). Switzerland, by adopting the National cybersecurity strategy, demonstrates how to build stakeholders' confidence and how national competitiveness depends on institutional risk maturity (Federal Council, 2023). The strategy values stakeholder trust in Swiss institutions' cybersecurity capability to preserving Switzerland's status as a leading financial and business hub (Federal Council, 2023). FINMA Circular 2023/1 established requirements for operational risk that call for advanced risk-management skills (FINMA, 2022).

The Swiss National Cyberstrategy's investment approach to cybersecurity in Switzerland reflects its understanding of the economic benefits of mature risk management for individuals and organizations, particularly for the national economy (Federal Council, 2023). This approach underscores how investments in the maturity of cybersecurity risk management yield returns by reducing incident costs, enhancing competitiveness, and improving economic resilience (Federal Council, 2023; Durst et al., 2024). FINMA emphasizes risk-based governance and operational-resilience capabilities in the Swiss banking sector (FINMA, 2022).

4.4. Measurement of cybersecurity risk maturity

Cybersecurity risk maturity assessment helps organizations systematically evaluate cybersecurity capabilities, identify opportunities for improvement, and demonstrate regulatory compliance (Brezavšček & Baggia, 2025; Büyüközkan & Güler, 2025). Today, measurement methods employ advanced tools and frameworks that account for multiple dimensions of cybersecurity risk maturity and generate actionable information to support organizational improvement (Burch et al., 2024; Durst et al., 2024; Lallie et al., 2021). The development of measurement approaches reflects the evolution of cybersecurity threats and the recognition that successful risk management requires systems capable of systematic assessment and iterative improvement (Brezavšček & Baggia, 2025; Büyüközkan & Güler, 2025; Sarker, 2022). International regulatory and standards frameworks establish cybersecurity and resilience requirements against which organizations can assess compliance and improvement needs (European Parliament and Council of the European Union, 2022a; European Union, 2024; NIST, 2024). Widely used cybersecurity frameworks include the NIST Cybersecurity Framework, whose Profiles and Implementation Tiers help organizations describe current and target cybersecurity outcomes and the rigor of risk-governance practices (NIST, 2024). The measurement approach of the framework, in its latest version CSF 2.0, uses 6 core functions (Govern, Identify, Protect, Detect, Respond, Recover) and includes 22 categories followed by

106 subcategories, where organizations can evaluate their capabilities within a systematic and comprehensive framework and identify the main areas where the model could be improved (NIST, 2024). The implementation tiers of the NIST Cybersecurity Framework provide an organized way to measure organizational maturity across 4 levels: Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4) (Azmi et al., 2018; NIST, 2024). Each tier represents a higher level of risk management, enabling the organization to assess whether it is currently at the appropriate level and whether it wishes to make changes (NIST, 2024). The measurement method focuses on self-assessment potential for guidance to third parties and on continuous monitoring (NIST, 2024).

The Cybersecurity Maturity Model Certification is a critical measurement framework for defense contractors and organizations handling Controlled Unclassified Information (U.S. Department of Defense, 2022). The Cybersecurity Maturity Model Certification 2.0 measurement approach comprises three maturity levels (Foundational, Advanced, Expert). It aligns with the security requirements outlined in NIST SP 800-171 across 14 domains (U.S. Department of Defense, 2022). With their focus on objective assessment criteria and independent validation, the framework's measurement methodology ensures consistent and reliable maturity assessments across the defense industrial base (Li, 2018; Sarker, 2022). Several European Union (EU) measurement frameworks have introduced holistic approaches to assessing cybersecurity risk maturity levels, notably through NIS2 (European Parliament and Council of the European Union, 2022b) and DORA (European Parliament and Council of the European Union, 2022a). The NIS2 Directive specifies metrics for essential and important entities across 18 sectors, including risk management, incident response and handling, business continuity, and supply chain protection (European Commission, 2023). Although it aims to harmonize standards across EU member states, the directive permits national transposition and, at its core, sets out measures that emphasize proportionality and sector-specific requirements (European Commission, 2023).

DORA offers measurement frameworks for banks and ICT service providers in the EU (European Parliament and Council of the European Union, 2022a). The framework emphasizes regular monitoring and testing of ongoing resilience capabilities to ensure a continuous state of digital operational resilience (European Parliament and Council of the European Union, 2022a). Global standards organizations have developed rigorous measurement frameworks to provide internationally applicable methods for evaluating cybersecurity risk maturity (European Commission, 2023; European Parliament and Council of the European Union, 2022a). The

ISO/IEC 27001:2022 standard provides a framework for information security management systems, specifying security controls across four themes: organizational, people, physical, and technological (ISO, 2022b). Measurements methodology within the standard stresses process maturity and continuous improvement with periodic surveillance audits and triennial recertification (ISO, 2022b). Self-assessment capabilities are the focus of the measurement approach, with regular third-party validation, enabling organizations to deliver continuous improvement while reducing assessment burden (Humphreys, 2008). FINMA has implemented advanced measurement frameworks for financial intermediaries that integrate cyber risk maturity and operational risk management (FINMA, 2022).

Precise measurement of cybersecurity risk maturity is best achieved through systematic approaches, rigorous methodologies, and continuous improvement principles, thereby enabling an organization to develop sound, actionable, and sustainable assessment capability (NIST, 2020; ISO, 2022b). Most approaches and best practices yield higher accuracy and greater utility in cybersecurity risk maturity assessments and address common challenges (NIST, 2020; CISA, 2023a), as evidenced by the available literature and experience. These practices align technical expertise, organizational experience, and methodological competence with the required measurement programs (ISO, 2022b; NIST, 2020). The selection and integration of any of these frameworks will establish a basic best practice, as it will include all aspects of cybersecurity risk maturity (European Commission, 2023; European Parliament and Council of the European Union, 2022a). Companies should select measurement schemes that align with regulatory compliance requirements, business needs, and the organizational environment, and that fully capture the technical, organizational, and strategic dimensions (Federal Council, 2023; FINMA, 2024).

Risk-based prioritization and scoping are essential best practices that enable firms to orient their measurement toward critical and high-risk cybersecurity activities (NIST, 2024; ISO, 2022b). Appropriate measurement programs focus their assessments on business criticality, threat exposure, and regulatory requirements rather than measuring everything the same way (NIST, 2024). It helps organizations increase the value of investment in measurement while balancing resource challenges (Brezavšček & Baggia, 2025). Multi-source data collection and validation are important best practices that can improve the accuracy and reliability of measurement results (ISO, 2022b). Good measurement programs employ multiple measures, each incorporating automatic monitoring systems, document reviews, interviews, and direct observations (Sánchez-García et al., 2023). Cross-validation helps identify discrepancies and

knowledge gaps, leading to a more holistic and accurate evaluation of the findings (Büyüközkan & Güler, 2025). They should also establish clear, objective criteria for assessing cybersecurity capabilities and use standardized approaches to ensure neutrality and minimize subjectivity and bias (Brezavšček & Baggia, 2025). Structured assessment guides and consistent evidence requirements can improve the repeatability of resilience assessments (CISA, 2020; Federal Office for National Economic Supply, 2023). Independent third-party validation and third-party assessment are considered effective means of enhancing the credibility and accuracy of evaluation results (ISO, 2022b).

Sector-specific methods are set out in the DORA to evaluate the maturity of cyber risk management among financial institutions (European Commission, 2023; European Parliament and Council of the European Union, 2022a). This approach links cybersecurity assessment to all aspects of operational resilience, including ICT risk management, business continuity, and third-party risk management (European Commission, 2023; European Parliament and Council of the European Union, 2022a). Organizational resilience capacities are assessed using quantitative measures, qualitative evaluation, and scenario-based testing within the assessment toolkit (European Commission, 2023). Verification of assessment results is carried out through supervisory reviews and on-site examinations (European Commission, 2023; European Parliament and Council of the European Union, 2022a). The evaluation of the Swiss ICT Minimum Standards Assessment Methodology is conducted through self-assessment questionnaires, document reviews, and periodic third-party verification (Federal Office for National Economic Supply, 2023). The framework is straightforward, provides clear references to evidence requirements and assessment guidelines, and reduces the administrative burden (Federal Office for National Economic Supply, 2023).

FINMA has integrated cybersecurity risk into its broader operational risk management framework, focusing on governance, risk identification, risk mitigation, and risk monitoring (FINMA, 2022). The assessment process comprises risk-based evaluation, supervisory review, and on-site examination to ensure that operational risks are effectively covered (FINMA, 2022). The approach focuses on proportionality and risk-based strategies that match assessment intensity and institutional risk profiles (FINMA, 2022). Industry-specific assessment methodologies provide tailored approaches to cybersecurity risk maturity assessment and measurement based on sector-level requirements and risks (Brezavšček & Baggia, 2025). Healthcare cybersecurity must account for patient safety and medical-device and health-data security risks (Allen, 2023; Yan et al., 2023).

Energy sector organizations employ measures to protect critical infrastructure, ensure compliance with the North American Electric Reliability Corporation CIP, and secure operational technology, thereby safeguarding the energy sector (Business Continuity Institute, 2024). This type of sector-specific initiative illustrates how a general measurement framework can be adapted to the diverse requirements of different sectors (ISO, 2022b).

Previous research on cybersecurity risk maturity

In line with the ever-evolving threat landscape, the field of cybersecurity risk maturity has become an imperative area of research for more specialized approaches to building organizational-wide cybersecurity capability maturity. Recent research on information and cybersecurity maturity assessment shows growth in sector-specific models, lightweight approaches for SMEs, and methods incorporating emerging technologies. Brezavšček and Baggia (2025) reviewed 96 studies published between 2012 and 2024 and identified continuing implementation challenges related to model complexity, insufficient sector-specific customization, and limited organizational resources.

Cheimonidis and Rantos (2023) note that conventional, periodic risk assessments are ill-suited to rapidly changing threat environments; consequently, dynamic risk assessment approaches, which enable continuous, real-time analysis of the organizational security posture, have become popular. This development mirrors the overall paradigm in which cybersecurity organizations are moving - away from reactive, compliance-driven efforts, and towards proactive, risk-based models and, importantly, adaptive capability building. The academic literature shows considerable diversity in theoretical frameworks for cybersecurity maturity, ranging from prescriptive models that specify capabilities to descriptive models that capture the dynamics of organizational development. This diversity was evident in research by Büyüközkan and Güler (2025), which highlighted the complexity of cybersecurity threats and the organizational context in which security capability building and maintenance occur. The most recent systematic literature reviews identified more than 50 cybersecurity maturity models—each demonstrating distinct aspects of organizational security capability development and use while employing diverse assessment methodologies (Brezavšček & Baggia, 2025). The inclusion of behavioral and organizational factors represents a particularly meaningful theoretical advancement in cybersecurity maturity research. Jalali et al. (2019) demonstrated, through extensive simulations, that traditional assumptions about rationality in cybersecurity investments are frequently violated, with both experienced and inexperienced users exhibiting

systematic bias in their capability development decisions. This approach has far-reaching implications for the design of maturity models, underscoring the importance of models grounded in cognitive constraints, organizational limitations, and behavioral factors that affect the development of security capabilities.

The overall comparison of international frameworks (e.g., NIST CSF, NIS2, DORA) highlights a major paradigm shift: institutions are under unprecedented legal and strategic pressure to demonstrate and maintain cyber maturity. Consequently, this chapter has repositioned cyber resilience beyond a static IT compliance checklist to a strategic capability emerging within holistic risk governance. Having developed this essential premise, the following chapter shifts its focus to empirical validation. It discusses the structural research framework and the central methodology developed to formally evaluate the hypothesized effects of risk maturity on resilience outcomes.

5. EMPIRICAL RESEARCH OF THE CONNECTION OF CYBERSECURITY RISK MATURITY AND RESILIENCE IN BUSINESS

This chapter presents an empirical examination of the proposed capability–governance model, linking cybersecurity risk maturity to organizational resilience in large Swiss enterprises. It specifies the research design, measurement approach, and analytical procedures applied to test hypotheses on how governance, collaboration, internal capabilities, and environmental turbulence jointly shape maturity and, in turn, resilience. The chapter then presents descriptive results, assesses the measurement model, and evaluates the structural relationships using structural equation modeling.

5.1. Methodology

This empirical study was designed to test an integrated capability–governance model that explains how cybersecurity risk maturity contributes to organizational resilience in large Swiss enterprises. Before the main survey, a pilot study comprising semi-structured interviews with Swiss CISOs and IT leaders was conducted to refine the conceptual framework and ensure the relevance of the items. These interviews supported clarity in conceptual framing, the intelligibility of items, and their relevance to practice. These expert contributions informed refinements in wording and alignment of items with real-world cybersecurity governance practices. Additionally, written feedback from practitioners was collected to ensure consistent interpretation of constructs and to mitigate response bias. Pilot testing with 10 senior executives employed a two-phase approach. In addition to written feedback, individual cognitive interviews were implemented with the ‘think-aloud’ protocol (30–45 minutes each). This method provided participants with a platform to express their thoughts as they responded, enabling identification and addressing potential sources of measurement error or comprehension issues before the main study. Data were collected through a structured questionnaire administered to respondents with organizational oversight and cybersecurity competence, including board members, cybersecurity leaders, IT managers, and other relevant professionals. The hypotheses were evaluated using structural equation modeling in JASP 0.19.3.

The proposed model in Figure 1 integrates organizational, technological, and governance-related determinants to explain differences in cybersecurity risk maturity and, ultimately,

organizational resilience. The model tests cascading logic in which top management's risk perception and support facilitate external collaboration, which in turn strengthens internal capabilities, ultimately driving cybersecurity risk maturity and resilience. Market and technological turbulence are incorporated to reflect environmental dynamism and to test whether external conditions shape managerial risk perceptions and maturity outcomes. The following sections describe the research design, measurement approach, and analytical procedures used to empirically evaluate the model.

5.1.1. Research instrument

Table 5 presents the research instrument used to operationalize the study's latent constructs through a structured questionnaire. All constructs are measured with reflective indicators on a seven-point Likert scale (1 = strongly disagree to 7 = strongly agree), capturing respondents' perceptions of their organization. Organizational resilience (R) is measured using three items: business continuity plans (R1), rapid adaptation (R2), and systematic integration of lessons (R3). In comparison, the cybersecurity risk maturity (CSRM) is captured across three items: risk identification (CSRM1), mitigation and control (CSRM2), and monitoring and reporting (CSRM3), spanning the cyber risk lifecycle (Rajan et al., 2021). In addition, the instrument applies three to four items per construct to other constructs, such as technological infrastructure (TI) (Van Laak, 2004), cybersecurity resources and capabilities (CSRC) (Rajan et al., 2021), cybersecurity awareness (CSA) (Dash & Ansari, 2022), cybersecurity training (CST) (Hatzivasilis et al., 2020), and cybersecurity alliance and collaboration (CSAC) (He et al., 2017; Verma et al., 2025). Finally, the model includes top management support for cybersecurity (CSTMS) and top management risk perception (CSTMRP) (Sonnenschein et al., 2017) as governance-related antecedents, alongside market turbulence (MT) and technological turbulence (TT) (Jaworski & Kohli, 1993; Bodlaj & Čater, 2019; Kilani, 2020), to capture external environmental dynamism.

Table 5: Research instrument

Latent Variable	Definition	Questions (Likert scale 1-7)
Resilience (R)	Resilience refers to the fundamental ability to anticipate, prepare for, respond to, and recover from disruptive incidents, as well as the capacity to maintain services amid challenges and adjust to given situations (Federal Council, 2023; ISO, 2019). Contemporary literature indicates that resilient organizations possess dynamic capacities that enable them to absorb shocks, adapt to new conditions, and strengthen themselves in the aftermath of adversity through ongoing learning and strategic transformation (Liu et al., 2024; Jiang et al., 2019). The notion has evolved, shifting from undifferentiated, recovery-oriented approaches to holistic models that encompass the technical, organizational, and strategic dimensions of adaptive capacity (Federal Council, 2023). These capabilities are consistent with national cybersecurity strategies, including the Swiss National Cyberstrategy (NCS) 2023–2027 (Federal Council, 2023) and the NCSC ICT Minimum Standard (Federal Office for National Economic Supply, 2023).	R1. Our organization has robust business continuity plans in place to manage the impact of cybersecurity incidents and keep our critical activities functioning. R2. Our organization demonstrates rapid adaptation of cybersecurity strategies and processes in response to changes in the threat landscape. R3. Our organization systematically learns from past cybersecurity incidents and integrates lessons learned into improved security practices.
Cybersecurity Risk Maturity (CSRM)	Cybersecurity Risk Maturity is an organization's sophisticated and systematic approach to recognizing, identifying, evaluating, managing, and improving its ability to manage cybersecurity risk across all organizational levels and functions (Rabii et al., 2020; NIST, 2024; ISO, 2022a). This concept encompasses risk governance tools, advanced threat intelligence, and risk assessment	CSRM 1. Our organization has established procedures in respect of the identification and assessment of cybersecurity risks. CSRM 2. Our organization implements effective

Latent Variable	Definition	Questions (Likert scale 1-7)
	techniques, coupled with continuous monitoring (NIST, 2024; European Parliament and Council of the European Union, 2022a), thereby enabling organizations to proactively mitigate evolving cyber threats. Mature organizations tend to exhibit a holistic approach for covering entire risk management lifecycles that align with international standards, such as, for example, the NIST Cybersecurity Framework, (NIST, 2024), ISO/IEC 27001:2022 (ISO, 2022b), and the NCSC ICT Minimum Standard (Federal Office for National Economic Supply, 2023), while maintaining continuous improvement processes (COSO, 2017).	cybersecurity risk mitigation and control measures. CSRM 3. Our organization has comprehensive monitoring of cyber risks with reporting to leadership.
Technological Infrastructure (TI)	Technological infrastructure comprises the broad physical, software, network, cloud, and digital platform environments on which an organization's operations and cybersecurity capabilities are based (NIST, 2024; ISO, 2019). The current technological architecture should encompass modern security approaches, including defense-in-depth, zero trust, AI, and resilience methodologies that are adaptable to dynamic threat landscapes without adversely affecting operations (NIST, 2020; NIST, 2024). In particular, Swiss organizations benefit from a strong technological backbone, which aligns with the National Cybersecurity Strategy (Federal Council, 2023), the NCSC ICT Minimum Standard (Federal Office for National Economic Supply, 2023), and FINMA	TI 1. Our organization maintains a robust and secure technological infrastructure. TI 2. Our organization operates integrated and scalable technology systems. TI 3. Our organization deploys advanced cybersecurity tools and technologies.

Latent Variable	Definition	Questions (Likert scale 1-7)
	Circular 2023/1 on critical infrastructure protection (FINMA, 2022).	
Cybersecurity Resources & Capabilities (CSRC)	Cybersecurity resources and capabilities encompass a comprehensive suite of human capital, technology assets, financial investments, and organizational processes required to effectively address cybersecurity needs and enhance resilience (NIST, 2020; ISACA, 2022). The framework encompasses personnel, including cyber specialists, as well as sophisticated security products, threat intelligence mechanisms, incident response solutions, and continuous learning opportunities that augment an organization's security posture (Paulsen et al., 2012; (ISC)², 2023). Modern business requires positioning cybersecurity resources in line with international guidance, for instance, the NIST Cybersecurity Framework and the EU NIS2 Directive (European Commission, 2023), while addressing Swiss regulations, e.g., FINMA Circular 2023/1 (FINMA, 2022), in addition to the intent of the Swiss National Cybersecurity Strategy (Federal Council, 2023).	CSRC1. Our organization maintains skilled cybersecurity employees. CSRC 2. Our organization maintains effective cybersecurity technology and tool capabilities. CSRC 3. Our organization allocates cybersecurity budget and resources effectively.
Cybersecurity Awareness (CSA)	Cybersecurity awareness refers to the foundational knowledge and understanding that an employee has about cybersecurity threats, vulnerabilities, and defensive and preventive techniques within their organization's cybersecurity domain (Arbanas et al., 2021; European Union Agency for Network and Information Security, 2018). It is an	CSA 1. Our organization provides employees with effective cybersecurity knowledge and understanding. CSA 2. Our organization fosters a strong cybersecurity

Latent Variable	Definition	Questions (Likert scale 1-7)
	integrated model that covers cognitive and cultural aspects across domains within the cyber domain, such as threat identification, security-aware behaviors, and the embedding of cybersecurity factors into their work (Da Veiga & Martins, 2015; Alshaikh, 2020). Awareness initiatives must be driven by continuous communication and visible leadership commitment across all functional areas. Furthermore, fostering a non-punitive incident-reporting culture is essential for embedding security into everyday behaviors, aligning specifically with the NCSC ICT Minimum Standard (Federal Office for National Economic Supply, 2023) and established security awareness frameworks (Arbanas et al., 2021).	culture and employee engagement. CSA 3. Our organization's employees demonstrate awareness of cybersecurity threats and best practices in their daily work.
Cybersecurity Training (CST)	Cybersecurity training encompasses all organized training programs and skill-building activities that enhance employees' cybersecurity knowledge, technical skills, and behavioral responses to cyber threats (Paulsen et al., 2012). This encompasses role-based training tracks, competency-based assessment frameworks, simulation-based learning environments, and ongoing professional development programs designed to cultivate specific cybersecurity skills and knowledge (ISO, 2022a). Cybersecurity training programs that demonstrate measurable improvements in cybersecurity performance in accordance with the requirements outlined in the NIST NICE Framework, align with adult learning principles, comply with applicable regulations such as	CST 1. Our organization has comprehensive and effective cybersecurity programs. CST 2. Our organization provides effective cybersecurity skill development and competency building. CST 3. Our organization's cybersecurity training program is continuously improved based on formal assessments.

Latent Variable	Definition	Questions (Likert scale 1-7)
	ISO/IEC 27001:2022, and address Swiss-specific multilingualism must be developed (NIST, 2024; Federal Council, 2023).	
Cybersecurity Alliance and Collaboration (CSAC)	Cybersecurity alliances and collaboration are strategic partnerships, information-sharing initiatives, and collective defense systems that enable organizations to share intelligence, resources, and skills to improve cybersecurity effectiveness through coordinated activities (Assibi, 2023). Contemporary collaboration models include public-private partnerships, industry consortia, threat intelligence sharing platforms, and cross-sector coordination mechanisms that integrate with international efforts, such as the EU Computer Security Incident Response Team networks, US CISA partners, and the Swiss Federal Office for Cybersecurity (BACS) coordination program (Federal Council, 2023). Successful collaboration depends on complex governance structures, shared communication protocols, and trust-building to facilitate the safe sharing of information while protecting competitive interests (European Union Agency for Network and Information Security, 2018; European Parliament and Council of the European Union, 2022a).	CSAC 1. Our organization demonstrates effective cybersecurity partnerships and development. CSAC 2. Our organization exhibits effective cybersecurity information sharing and intelligence collaboration. CSAC 3. Our organization participates actively in industry-wide cybersecurity initiatives.
Cybersecurity Top Management Support (CSTMS)	Cybersecurity top management support refers to the dedicated attention, resource commitment, engagement, and strategic direction provided by senior leaders and the board of directors to ensure	CSTMS 1. Our organization's top management demonstrates a strong commitment to

Latent Variable	Definition	Questions (Likert scale 1-7)
	that the organization develops, maintains, and advances its cybersecurity proficiency (Rothrock et al., 2018; economiesuisse, 2023). Current research indicates that promoting effective top management support necessitates attention to cybersecurity risks, alignment with business strategy, overseeing governance structures, and investing in cybersecurity activities that support regulatory compliance (e.g., the SEC cybersecurity disclosure rules, the EU NIS2 Directive (European Parliament and Council of the European Union, 2022a), and FINMA Circular 2023/1 (FINMA, 2022). Swiss firms specifically benefit from this top-management support, which is also informed by the Swiss National Cybersecurity Strategy (Federal Council, 2023), industry-specific needs, and international best practices within extensive governance frameworks (NIST, 2024).	cybersecurity and effective resource allocation. CSTMS 2. Our organization's leadership exhibits effective cybersecurity governance and oversight. CSTMS 3. Our organization's top management ensures accountability for cybersecurity performance.
Cybersecurity Top Management Risk Perception (CSTMRP)	Cybersecurity Top Management Risk Perception refers to the senior managers' knowledge, judgment, cognitive appraisal of cybersecurity threats and vulnerabilities, and their potential impact on organizational goals and stakeholder value (COSO, 2017; NIST, 2024). Current studies show that senior management needs an accurate perception of risk to allocate resources appropriately, plan strategically, and build resilience, in line with guidelines such as COSO's Enterprise Risk Management (COSO, 2017), NIST's Risk Management Framework, and the	CSTMRP 1. Our organization's top management demonstrates an accurate understanding of cybersecurity risk assessment. CSTMRP 2. Our organization's senior leadership exhibits effective cybersecurity threat

Latent Variable	Definition	Questions (Likert scale 1-7)
	Risk Management Standards (ISO, 2022a). Risk sensitivity requires organizations to integrate cyber threat intelligence and contextual information into risk assessment and to consider stakeholder expectations and legal and regulatory requirements in cybersecurity risk management (Kure et al., 2022; National Institute of Standards and Technology, 2024).	awareness and intelligence utilization. CSTMRP 3. Our organization's executives make decisions with a comprehensive awareness of cyber risks.
Market Turbulence (MT)	Market turbulence is a dynamic environmental condition characterized by rapid shifts in customer preferences, competitive dynamics, regulatory demands, and economic conditions, resulting in uncertainty and requiring organizations to adapt (Liu et al., 2024; Jiang et al., 2019). Today's market volatilities are steered, among others, by digitalization and globalization, regulations such as the GDPR and Swiss laws on data protection, and new technologies that open up both chances and cybersecurity risks (European Parliament and Council of the European Union, 2016; Federal Assembly of the Swiss Confederation, 2023). Swiss companies face market turbulence due to the application of foreign financial services regulations, international compliance requirements, and the country's status as a global business hub, all of which demand a versatile policy response (FINMA, 2024; Federal Council, 2023).	MT 1. Our organization operates in an unpredictable, rapidly changing market. MT 2. Our organization faces frequent and intense competitive threats and market disruptions. MT 3. Our organization experiences external stakeholder pressure and conflicting demands (e.g., from regulators vs. customers).
Technological Turbulence (TT)	Technological turbulence refers to rapid changes in technology, the adoption of innovative	TT 1. Our organization operates in a rapidly

Latent Variable	Definition	Questions (Likert scale 1-7)
	solutions, particularly digital forms, and digital transformation pressures and innovation cycles that create both opportunities and risks for cybersecurity for organizations (NIST, 2024). Current technological upheavals involve the integrated use of AI, the use of the cloud, deployment of the Internet of Things, and the development of quantum computing that necessitates such risk management and adaptation plans meeting orientations such as the NIST Cybersecurity Framework, the EU Cyber Resilience Act (European Union, 2024) and the Swiss National Cybersecurity Strategy (Federal Council, 2023; FINMA, 2024). Enterprises must weigh innovation opportunities against security risks, while ensuring that legal and regulatory compliance scales with them.	evolving and unpredictable technological environment. TT 2. Our organization experiences complexity in integrating and managing multiple emerging technologies. TT 3. Our organization faces pressure to rapidly adopt new technologies to remain competitive.

Source: Author's work

In addition to the latent-construct items reported in Table 5, the questionnaire contains several contextual blocks that support interpretation of the structural model and enable robustness checks. First, each Likert-type construct item is accompanied by brief "benchmark controls" that provide respondents with practical reference points (e.g., business continuity targets, incident response practices, risk register and reporting, infrastructure resilience, role-based training, and threat intelligence sharing). These benchmarks are intended to reduce variation in interpretation across respondents and to anchor responses in observable organizational practices rather than in abstract self-assessment.

For example, the Benchmark Controls for R1 ("Our organization has robust business continuity plans in place to manage the impact of cybersecurity incidents and keep our critical activities functioning") are defined as follows:

- Business continuity architecture - 100% of critical business functions have documented backup systems, alternative processes, and recovery procedures, with RTO and RPO that are determined by the business impact analysis based on the organizational criticality and not fixed timeframes.
- Incident containment - All cyber incidents are contained according to documented incident response procedures with defined containment strategies appropriate to the incident type and severity, following incident response guidelines for effective containment, eradication, and recovery.
- Operational resilience - Organization maintains documented service delivery targets during disruptions based on business impact analysis and regulatory requirements, with evidence of successful resilience testing and validation.

Benchmark controls for all research items are provided in Annex 1.

Second, the instrument includes a "Cybersecurity Events and Measures" section capturing factual organizational conditions and recent experience: whether the organization faced a significant cybersecurity incident within the last 24 months (and, if yes, the primary impact), whether formal cybersecurity assessments are conducted (regularly or on an ad hoc basis), how security monitoring is organized (internal unit, outsourced function, ad hoc team, or none), whether annual awareness training is provided (mandatory, role-specific, optional, or not provided), whether a business continuity plan exists and is tested, and how third-party cybersecurity risk is managed (formal program/framework, contract clauses, informal approach, or no plan/tool). These items provide operational controls for maturity and resilience and enable subgroup and sensitivity analyses (e.g., comparing organizations with and without recent incidents or with mature monitoring arrangements).

Finally, a demographic block captures respondent and organizational descriptors used to contextualize findings and assess sample heterogeneity, including the respondent's role/title and tenure in the role, the organization's industry sector, approximate number of employees, the extent of operations abroad, and whether the organization belongs to a corporate group. Together, these non-latent questions strengthen external validity and support additional analyses, such as industry- and size-based comparisons, as well as checks for systematic differences related to international exposure or group membership.

5.1.2. Population and sample

The empirical study included a preparatory phase in which the questionnaire was pilot tested to assess respondents' comprehension of the questions and identify potential ambiguities. Based on pilot feedback, ambiguous wording was refined prior to the main data collection. The final questionnaire, consisting of statements adapted from established measurement scales in the literature, was administered via Google Forms and distributed via email. Invitations and follow-up reminders were sent to increase participation, targeting respondents with adequate organizational oversight and cybersecurity competence, primarily board-level representatives, heads of information technology, and other relevant professionals with knowledge and experience in cybersecurity governance. 500 email invitations were sent twice (initial invitation and reminder), followed by direct outreach to 1,000 executives via LinkedIn, also conducted twice to increase participation and ensure adequate representation of senior decision-makers. Data was collected anonymously, and the confidentiality of the information provided was ensured; codes were used solely for research administration and were accessible only during data analysis.

The final dataset comprised 170 completed responses. This corresponds to a response rate of approximately 11% relative to the 1,500 organizations contacted. Based on the Structural Statistics of Enterprises (STATENT) 2023 of the Swiss Federal Statistical Office, businesses in Switzerland are organized by size according to their employees (in full-time equivalents): micro-enterprises (1–9 employees), small (10–49 employees), medium (50–249 employees), and large (250 or more employees). The target population for this research comprises large enterprises operating within the Swiss jurisdiction. A detailed list of firms eligible for registration was compiled prior to the survey's publication, ensuring that the sampling approach adhered to rigorous methodological standards for respondent suitability and organizational eligibility. The STATENT reporting period 2023 showed 643,317 active enterprises in Switzerland (Swiss Federal Statistical Office, 2023). In the market economy sector, the census revealed 626,033 active enterprises, including 1,814 classified as large enterprises (representing approximately 0.29% of the overall market-active population). This means that these 1,814 companies constitute the formal population frame for the survey in this study, serving as the basis for analyzing the impact of cybersecurity risk maturity on organizational resilience in the country's most challenging corporate environments.

5.1.3. Statistical analysis

The data analysis was conducted in four phases. First, the sample characteristics were examined to address demographic considerations using descriptive statistics.

Second, the manifest variables were analyzed using descriptive statistics. The mean, standard deviation, and coefficient of variation were calculated for each manifest variable. The manifest variable values were also presented graphically.

Third, the instrument's validity was assessed using confirmatory factor analysis. JASP 0.19.3 was used for this purpose, and model parameters were estimated using the maximum likelihood estimator. The use of maximum likelihood estimation enabled simultaneous estimation of factor loadings, latent-variable variances and covariances, and measurement error terms by identifying the parameter values that maximize the likelihood of reproducing the observed covariance structure under the specified measurement model.

The pilot interviews and expert assessments were incorporated into the measurement validation process prior to conducting any formal statistical analyses. Qualitative feedback from CISOs and senior cybersecurity practitioners was also a valid source of input, confirming that the latent constructs were conceptually coherent and that the indicators aligned with the intended theoretical domain. Their comments helped refine the wording, remove redundancies, and ensure alignment with current cybersecurity governance frameworks (e.g., NIST CSF 2.0, ISO/IEC 27001:2022, and the Swiss National Cybersecurity Strategy). In addition, pilot feedback confirmed that respondents interpreted the constructs consistently, thereby reducing measurement error and enhancing the reliability of the latent variables used in confirmatory factor analysis and subsequent structural equation modeling.

A set of observable indicators represented each phenomenon (variable). Using confirmatory factor analysis, the measurement model's latent variables were extracted. During the evaluation of the measurement model, the following steps were performed: (i) assessment of the measurement model’s representativeness, (ii) calculation of representativeness measures, and (iii) assessment of the validity of the latent constructs.

The following latent constructs were used in the analysis:

- Resilience (R),
- Cybersecurity Risk Maturity (CSRM),
- Technological Infrastructure (TI),

- Cybersecurity Resources and Capabilities (CSRC),
- Cybersecurity Awareness (CSA),
- Cybersecurity Training (CST),
- Cybersecurity Alliance and Collaboration (CSAC),
- Cybersecurity Top Management Support (CSTMS),
- Cybersecurity Top Management Risk Perception (CSTMRP),
- Market Turbulence (MT), and
- Technological Turbulence (TT).

Factor loadings were calculated for each manifest variable, and indicators with loadings below 0.4 were removed from the analysis.

Fourth, structural equation modeling (SEM) was used to test the study's hypotheses. The representativeness of the SEM model was examined using the CFI, RMSEA, and SRMR indices. SEM yielded a set of regression equations in which latent variables were specified as both dependent and independent variables. The estimated parameters of these equations, assessed by statistical significance at the 5% level, were used to determine whether each hypothesis was accepted or rejected.

The following procedures were used to test the hypotheses:

- If the estimated parameter for the independent latent variable Cybersecurity Risk Maturity (CSRM) in a regression equation with the dependent latent variable Resilience (R) was positive and statistically significant at the 5% level, hypothesis H1 was accepted; otherwise, it was rejected.
- If the estimated parameter for the independent latent variable Technological Infrastructure (TI) in a regression equation with the dependent latent variable Cybersecurity Risk Maturity (CSRM) was positive and statistically significant at the 5% level, hypothesis H2a was accepted; otherwise, it was rejected.
- If the estimated parameter for the independent latent variable Cybersecurity Resources and Capabilities (CSRC) in a regression equation with the dependent latent variable Cybersecurity Risk Maturity (CSRM) was positive and statistically significant at the 5% level, hypothesis H2b was accepted; otherwise, it was rejected.
- If the estimated parameter for the independent latent variable Cybersecurity Awareness (CSA) in a regression equation with the dependent latent variable Cybersecurity Risk

Maturity (CSRM) was positive and statistically significant at the 5% level, hypothesis H3a was accepted; otherwise, it was rejected.

- If the estimated parameter for the independent latent variable Cybersecurity Training (CST) in a regression equation with the dependent latent variable Cybersecurity Risk Maturity (CSRM) was positive and statistically significant at the 5% level, hypothesis H3b was accepted; otherwise, it was rejected.
- If the estimated parameter for the independent latent variable Cybersecurity Alliance and Collaboration (CSAC) in a regression equation with the dependent latent variable Technological Infrastructure (TI) was positive and statistically significant at the 5% level, hypothesis H4a was accepted; otherwise, it was rejected.
- If the estimated parameter for the independent latent variable Cybersecurity Alliance and Collaboration (CSAC) in a regression equation with the dependent latent variable Cybersecurity Resources and Capabilities (CSRC) was positive and statistically significant at the 5% level, hypothesis H4b was accepted; otherwise, it was rejected.
- If the estimated parameter for the independent latent variable Cybersecurity Alliance and Collaboration (CSAC) in a regression equation with the dependent latent variable Cybersecurity Awareness (CSA) was positive and statistically significant at the 5% level, hypothesis H5a was accepted; otherwise, it was rejected.
- If the estimated parameter for the independent latent variable Cybersecurity Alliance and Collaboration (CSAC) in a regression equation with the dependent latent variable Cybersecurity Training (CST) was positive and statistically significant at the 5% level, hypothesis H5b was accepted; otherwise, it was rejected.
- If the estimated parameter for the independent latent variable Cybersecurity Top Management Support (CSTMS) in a regression equation with the dependent latent variable Cybersecurity Alliance and Collaboration (CSAC) was positive and statistically significant at the 5% level, hypothesis H6 was accepted; otherwise, it was rejected.
- If the estimated parameter for the independent latent variable Cybersecurity Top Management Risk Perception (CSTMRP) in a regression equation with the dependent latent variable Cybersecurity Top Management Support (CSTMS) was positive and statistically significant at the 5% level, hypothesis H7 was accepted; otherwise, it was rejected.

- If the estimated parameter for the independent latent variable Market Turbulence (MT) in a regression equation with the dependent latent variable Cybersecurity Top Management Risk Perception (CSTMRP) was positive and statistically significant at the 5% level, hypothesis H8 was accepted; otherwise, it was rejected.
- If the estimated parameter for the independent latent variable Technological Turbulence (TT) in a regression equation with the dependent latent variable Market Turbulence (MT) was positive and statistically significant at the 5% level, hypothesis H9 was accepted; otherwise, it was rejected.
- If the estimated parameter for the independent latent variable Technological Turbulence (TT) in a regression equation with the dependent latent variable Cybersecurity Risk Maturity (CSRM) was negative and statistically significant at the 5% level, hypothesis H10 was accepted; otherwise, it was rejected.

This chapter specifies the empirical study's methodological foundations, including the conceptual research model, the hypothesized relationships, the operationalization of constructs through a structured questionnaire, the target population and the achieved sample, and the analytical strategy used to assess measurement quality and test the structural paths. The next chapter reports the empirical results, beginning with descriptive statistics and measurement model assessment, and subsequently presents the structural equation modeling findings and hypothesis-testing outcomes.

5.2. Results

This chapter presents the study's empirical findings and evaluates the proposed research model. It first presents the sample characteristics and descriptive evidence on cybersecurity risks and prevention practices, then assesses the measurement model, and finally reports the structural equation modeling results and hypothesis-testing outcomes.

5.2.1. Sample characteristics

Table 6 shows that the sample represents a broad cross-section of sectors, with the largest representation in information technology and cybersecurity (21.8%), followed by financial services (14.7%) and manufacturing/industrial organizations (14.1%). Healthcare and life sciences (9.4%) and retail/food/hospitality (8.2%) contribute additional heterogeneity, while energy/utilities, public sector, business services, and construction are present in smaller proportions. Overall, the distribution supports sectoral diversity for testing a generalizable model of cybersecurity risk maturity and resilience in large enterprises, while also indicating a

weighting toward sectors that are typically more digitally intensive and cyber-exposed (particularly information technology and financial services). This pattern should be considered when interpreting descriptive patterns and model estimates.

Table 6: Industry sector of respondent organization (coded from open-text responses; n = 170)

Industry sector category (coded)	N	%	Illustrative examples (as reported)
Information technology and cybersecurity	37	21.80%	IT; IT Service Partner; IT Dienstleistung (Eng. Information technology services)
Financial services (banking, insurance, payments)	25	14.70%	Financial Services; Finance; Insurance and Banking
Manufacturing, industrial, engineering	24	14.10%	Chemical, industry, commodity trade, and mining
Healthcare, pharma, life sciences	16	9.40%	Pharmacy; Healthcare; Health Care
Retail, food, hospitality	14	8.20%	Food; Retail; Food industry
Logistics, transportation, travel	9	5.30%	Logistics & Transportation; Mail-Order Company; Logistics
Other (too broad/ambiguous to code reliably)	9	5.30%	Computer Science; Second sector; Industry
Energy and utilities	8	4.70%	Utilities; Energy & Recycling; Energy
Business services (legal, consulting, human resources, business process outsourcing)	7	4.10%	Legal; BPO; Consulting
Public sector, education, research	7	4.10%	Public; Local government; Education

Construction and building materials	5	2.90%	Construction; building materials; construction and building materials industry
Not disclosed / unclear	4	2.40%	No Comment; (answer would disclose the company)
Media	3	1.80%	Media
Defense and security	2	1.20%	Defense; Military
Total	170	100.0%	

Source: Author's work

Table 7 reports descriptive statistics for organizational size measured by the number of employees. The sample includes 170 valid observations with no missing values, indicating complete reporting for this variable. The distribution of firm size is highly dispersed, as reflected in a large standard deviation relative to the mean (mean = 17,572.61; standard deviation = 68,169.23), with values ranging from 4,000 to 785,000 employees. This wide range suggests substantial heterogeneity on an organizational scale within the dataset and indicates that the employee variable is skewed by a small number of very large organizations. Because the smallest responding organization reports 4,000 employees, the sample achieved covers the upper segment of the population frame rather than its full range from 250 employees upward. Findings therefore generalize to very large Swiss enterprises.

Table 7: Descriptive statistics for the number of employees

Descriptive Statistics	# of employees
Valid	170
Missing	0
Mean	17,572.61
Std. Deviation	68,169.23

Minimum	4,000.00
Maximum	785,000.00

Source: Author's work

Table 8 indicates that the sample is skewed toward internationally exposed organizations: almost half of the respondents (44.7%) reported that at least one-quarter of their total revenue was generated abroad. A further 22.9% reported limited international exposure, while 32.4% operated exclusively within Switzerland. This distribution is relevant to interpretation because cross-border activity is typically associated with more complex operating environments (e.g., multi-jurisdictional regulatory requirements, more extensive supply chains, and broader threat exposure), which can influence both cybersecurity risk maturity and resilience-related practices.

Table 8: Extent of operations abroad, measured as share of total revenue from abroad (n = 170)

International exposure of the organization	n	%
Operations exclusively within Switzerland (0% revenue from abroad)	55	32.40%
Limited international exposure (<25% of total revenue from abroad)	39	22.90%
Significant international exposure (≥25% of total revenue from abroad)	76	44.70%
Total	170	100%

Source: Author's work

Table 9 indicates that the sample is relatively balanced with respect to group membership, with a slight predominance of organizations within a corporate group (52.4%). This is relevant for interpretation because group-affiliated firms often operate with shared governance structures, centralized security policies, and group-wide technology standards, which can influence both cybersecurity risk maturity and resilience-related practices. Conversely, standalone organizations may have greater autonomy but potentially more constrained resources or less standardization. The near-even split supports comparative and robustness analyses by enabling

meaningful contrasts between group and non-group organizations, should this variable be used as a control or for subgroup testing.

Table 9: Membership in a corporate group (GROUP variable; n = 170)

Organizational status	n	%
Part of a corporate group (GROUP = 1)	89	52.40%
Standalone / not part of a corporate group (GROUP = 0)	81	47.60%
Total	170	100.00%

Source: Author's work

Table 10 summarizes respondents' current roles/titles, derived from open-ended job descriptions. It indicates that the sample comprised predominantly participants with direct responsibility for or close involvement in information technology and cybersecurity governance and operations. A substantial share of respondents held senior executive positions (e.g., chief information officer, chief executive officer, and chief financial officer), as well as CISO and equivalent roles, suggesting that the dataset captures perspectives from organizational decision-makers responsible for risk prioritization, resourcing, and strategic oversight. In parallel, a large proportion of respondents reported IT/ICT management positions (such as head of information technology or head of infrastructure) and specialist technical roles (engineering, architecture, development, and operations), which strengthens the operational validity of responses related to technological infrastructure, controls, monitoring, and training. Overall, the role distribution supports the methodological assumption that respondents possessed the competence and organizational visibility required to provide informed assessments of cybersecurity risk maturity, its antecedents, and resilience-related practices within large enterprises.

Table 10: Respondent role category

Respondent role category (self-explanatory coding)	n	Share of sample	Illustrative examples (as reported)

Technical specialist roles (engineering, development, architecture)	32	18.80%	System Engineer; Platform Engineer; DevOps Engineer
C-suite / board executives (excluding CISO)	30	17.60%	Chief Information Officer; Chief Executive Officer; Chief Financial Officer
IT/ICT leadership and management (non-C-suite)	29	17.10%	Head of IT; Head of ICT; Director ICT
CISO and equivalents	28	16.50%	CISO; Global CISO; Group CISO
Business, operations, risk, or compliance management	16	9.40%	Head of Operational Risk; Group Compliance Officer; Senior Vice President Supply Chain
Cybersecurity or security specialist roles (non-CISO)	14	8.20%	Cybersecurity Analyst; IT Security Manager; Security Engineer
Consulting roles (IT/cyber/security)	8	4.70%	Security Consultant; Cybersecurity Consultant; Senior Consultant
Sales/account management	13	7.70%	Account Manager; Sales Director; Export Sales Manager
Total	170	100.0%	

Source: Author's work

Table 11 indicates that respondents reported approximately 6 years of experience in their current role, with substantial dispersion across the sample (standard deviation = 4.94). The range (1 to 22 years) suggests that the dataset includes both relatively new role-holders and long-tenured decision-makers, which is relevant for interpretation because tenure can influence awareness of security incidents, familiarity with organizational controls, and confidence in evaluating maturity and resilience practices.

Table 11: Respondent experience in current role (years) – descriptive statistics (EXPER_YRS; n = 170)

Descriptive statistic	Value
Valid	170
Missing	0
Mean	5.92
Std. Deviation	4.94
Minimum	1
Maximum	22

Source: Author's work

5.2.2. Cybersecurity risks and prevention practice

Respondents were asked if their organization experienced a significant cybersecurity incident in the past 24 months (Table 12). The results indicate that most respondents (65.9%) reported no significant cybersecurity incidents in the previous 24 months. Nevertheless, 14.7% of organizations confirmed at least one significant incident during this period, suggesting that material cyber events were not rare in the surveyed population. In addition, nearly one-fifth of respondents (19.4%) chose not to disclose their incident experience, which is noteworthy, as such non-disclosure may reflect confidentiality constraints, internal reporting policies, reputational concerns, or uncertainty about incident classification. Consequently, the combined share of confirmed incidents and non-disclosure (34.1%) suggests that incident exposure and/or sensitivity around incident reporting may be substantial among large enterprises, warranting consideration when interpreting subsequent model relationships.

Table 12: Experience of a significant cybersecurity incident in the past 24 months (n = 170)

Survey response: significant cybersecurity incident in the past 24 months	#	Structure in %
Confirmed: the organization experienced a significant incident	25	14.70%

No incident: the organization did not experience a significant incident	112	65.90%
Not disclosed: respondent preferred not to answer	33	19.40%
Total	170	100.00%

Source: Author's work

Among respondents who indicated a significant incident and described the primary impact (24 open-text responses), the impacts clustered into a small number of recurring themes. First, availability and operational disruption were prominent, ranging from general "availability" issues to explicit service denial and business interruption (for example, "Distributed Denial of Service attacks," "Denys services," "Interruption of all online activities," and "Kompletter Systemausfall während mehrerer Tage" (Eng. System outage lasting several days)). Second, ransomware and encryption-related disruptions recurred, including ransomware affecting legacy landscapes and localized encryption leading to knowledge or document loss (e.g., "Ransomware Attack of an outdated system landscape…," "knowledge loss due to encryption for one location," and "Ransomware").

Third, compromises of systems or platforms were reported (e.g., "Übernahme unseres Microsoft Tennants" (Eng. Takeover of our Microsoft tenant), "Messaging system hack," and "Attacker on internal server infrastructure"). Fourth, data-related consequences were noted, including third-party breaches and direct data loss (e.g., "data breach through third parties," "Data Loss," and "loss of documents such as billing documents"). Fifth, several responses pointed to social engineering and financial impacts (for example, "Fake phone calls from top mgr… loss of money," "Phishing," and a standalone "financial" impact). Finally, a minority of entries indicated limited or no direct impact, non-response/unclear text, or incidents outside the 24-month window (for example, "Nothing," "no direct impact, as we only supported…," and "Not in the last 24 months, but a ransomware incident in 2020").

Table 13 shows that most organizations conduct formal cybersecurity assessments regularly (71.2%), while 18.2% did so on an ad hoc basis. Only 3.5% reported not conducting assessments, and 7.1% of respondents were unsure whether assessments were performed.

Table 13: Formal cybersecurity assessments in the organization (n = 170)

Assessment practice	n	%
Conducted regularly (for example, annually)	121	71.20%
Conducted on an ad hoc basis	31	18.20%
Not conducted	6	3.50%
Respondent does not know	12	7.10%
Total	170	100%

Source: Author's work

Table 14 shows that security monitoring was most frequently organized through an internal formal unit or role (46.5%), followed by outsourced monitoring arrangements (31.2%). A smaller share relied on internal ad hoc teams (14.1%), while only 1.8% reported having no monitoring; 6.5% of respondents were unsure.

Table 14: Security monitoring arrangement (n = 170)

Monitoring arrangement	n	%
Internal formal unit/role (for example, SOC)	79	46.50%
External outsourcing (for example, outsourced SOC)	53	31.20%
Internal, ad hoc team	24	14.10%
No monitoring	3	1.80%
Respondent does not know	11	6.50%
Total	170	100%

Source: Author's work

Table 15 indicates that annual cybersecurity awareness training was predominantly mandated for all employees (77.1%). Smaller proportions reported mandatory training for specific roles (8.8%) or optional training (7.6%), while 4.1% reported no training and 2.4% did not know.

Table 15: Cybersecurity awareness training at least once per year (n = 170)

Training practice	n	%
Mandatory for all employees	131	77.10%
Mandatory for specific roles	15	8.80%
Optional	13	7.60%
Not provided	7	4.10%
Respondent does not know	4	2.40%
Total	170	100%

Source: Author's work

Table 16 shows that most organizations have a business continuity plan: 51.2% report regular testing, and 27.1% report that their plan has not been tested. A further 10.6% reported no formal plan (informal practices only), 2.4% reported no plan, and 8.8% were unsure.

Table 16: Business continuity plan (n = 170)

Business continuity planning status	n	%
Plan exists and is tested regularly	87	51.20%
Plan exists but is not tested	46	27.10%
No formal plan (informal practices only)	18	10.60%
No plan	4	2.40%
Respondent does not know	15	8.80%

Total	170	100%

Source: Author's work

Table 17 shows that third-party cybersecurity risk was most often managed via a formal program/framework (38.2%) or contract clauses (28.8%). An informal approach was reported by 12.4%, while 3.5% reported having no plan/tool; 17.1% of respondents did not know how third-party risk was managed.

Table 17: Management of third-party cybersecurity risks (n = 170)

Third-party cyber risk management approach	n	%
Formal program/framework	65	38.20%
Contract clauses only	49	28.80%
Informal approach	21	12.40%
No plan/tool	6	3.50%
Respondent does not know	29	17.10%
Total	170	100%

Source: Author's work

The evidence presented above suggests that the participating organizations generally reported established baseline cybersecurity governance practices, particularly periodic assessments, structured monitoring arrangements, and institutionalized awareness training. At the same time, the incident data and open-text descriptions indicate that disruptive events occur across multiple impact types, most notably availability disruptions, ransomware, data loss and compromises, and social engineering. The findings also indicate uneven maturity across specific domains, particularly in business continuity testing and third-party cyber risk management, where a substantial share of respondents reported informal approaches or limited visibility.

5.2.3. Level of cybersecurity maturity and its determinants

Table 18 reports descriptive statistics for the manifest indicators used to operationalize the latent constructs in the structural model (n = 170). The indicators are discussed in the following groups: (i) the outcome construct of organizational resilience (R), (ii) the core cyber capability of cybersecurity risk maturity (CSRM), (iii) internal technical and organizational enablers - technological infrastructure (TI) and cybersecurity resources and capabilities (CSRC), (iv) human and relational enablers - cybersecurity awareness (CSA), cybersecurity training (CST), and cybersecurity alliance and collaboration (CSAC), (v) governance-related constructs - cybersecurity top management support (CSTMS) and cybersecurity top management risk perception (CSTMRP), and (vi) environmental dynamism - market turbulences (MT) and technological turbulences (TT).

Table 18: Descriptive statistics for manifest variables

Indicator	n	Mean	Std. Deviation	Minimum	Maximum
R1	170	5.300	1.422	1	7
R2	170	5.165	1.392	1	7
R3	170	5.424	1.422	1	7
CSRM1	170	5.547	1.324	1	7
CSRM2	170	5.459	1.250	1	7
CSRM3	170	5.412	1.429	1	7
TI1	170	5.676	1.190	1	7
TI2	170	5.518	1.212	1	7
TI3	170	5.347	1.489	1	7
CSRC1	170	5.335	1.639	1	7
CSRC2	170	5.471	1.265	1	7
CSRC3	170	5.141	1.637	1	7

CSA1	170	5.382	1.439	1	7
CSA2	170	5.200	1.494	1	7
CSA3	170	5.153	1.337	1	7
CST1	170	5.147	1.400	1	7
CST2	170	4.876	1.496	1	7
CST3	170	4.941	1.549	1	7
CSAC1	170	5.071	1.490	1	7
CSAC2	170	4.924	1.569	1	7
CSAC3	170	4.659	1.741	1	7
CSTMS1	170	5.006	1.673	1	7
CSTMS2	170	4.976	1.602	1	7
CSTMS3	170	4.953	1.663	1	7
CSTMRP1	170	4.829	1.744	1	7
CSTMRP2	170	4.871	1.564	1	7
CSTMRP3	170	4.882	1.617	1	7
MT1	170	4.776	1.712	1	7
MT2	170	4.588	1.701	1	7
MT3	170	4.676	1.729	1	7
TT1	170	4.647	1.694	1	7
TT2	170	5.000	1.484	1	7
TT3	170	4.706	1.681	1	7

Source: Author's work

Organizational resilience (R) was assessed by evaluating the business continuity and adaptive security architectures, as well as post-incident learning capabilities. The mean values for all

three items were above the midpoint of the seven-point scale (R1: "Our organization has robust business continuity plans that maintain critical activities during cybersecurity incidents", M = 5.300; SD = 1.422; R2: "Our organization demonstrates rapid adaptation of cybersecurity strategies and processes in response to changes in the threat landscape.", M = 5.165; SD = 1.392; R3: "Our organization systematically integrates lessons from cybersecurity incidents into policies, processes, and training", M = 5.424; SD = 1.422). Within this block, the highest mean was observed for post-incident learning and continual improvement (R3), suggesting that post-incident debriefing and organizational learning were perceived as a stronger aspect of resilience than adaptive security architecture.

Cybersecurity risk maturity (CSRM) indicators were among the highest-rated in the instrument, indicating generally favorable self-assessments of cyber risk management capability. Respondents reported high evaluations for risk identification and methodology (CSRM1: "Our organization has established procedures in respect of the identification and assessment of cybersecurity risks", M = 5.547; SD = 1.324), control effectiveness and defense-in-depth architecture (CSRM2: "Our organization implements effective cybersecurity risk mitigation and control measures", M = 5.459; SD = 1.250), and continuous monitoring with risk metrics (CSRM3: "Our organization has comprehensive monitoring of cyber risks with reporting to leadership", M = 5.412; SD = 1.429). Dispersion was moderate, with the lowest variability for control effectiveness (CSRM2), suggesting relatively consistent perceptions across organizations regarding the effectiveness of security controls and the optimization of risk treatment.

Internal enablers exhibited a differentiated pattern. Technological infrastructure (TI) received the strongest ratings overall, particularly for infrastructure resilience and security architecture (TI1: "Our organization maintains a robust and secure technological infrastructure", M = 5.676; SD = 1.190; TI2: "Our organization operates integrated and scalable technology systems", M = 5.518; SD = 1.212), while next-generation security technology adoption was slightly lower and more heterogeneous (TI3: "Our organization deploys advanced cybersecurity tools and technologies", M = 5.347; SD = 1.489). Cybersecurity resources and capabilities (CSRC) were also rated above the midpoint but displayed higher dispersion than the technology items, pointing to greater cross-organizational differences in resourcing and capability development (CSRC1: "Our organization maintains skilled cybersecurity employees", M = 5.335; SD = 1.639; CSRC2: "Our organization maintains effective cybersecurity technology and tool capabilities", M = 5.471; SD = 1.265; CSRC3: "Our organization provides adequate financial

resources and investments for cybersecurity", M = 5.141; SD = 1.637). Notably, the variability for CSRC1 and CSRC3 was among the highest in the table, indicating substantial heterogeneity in perceived talent retention and funding adequacy of cybersecurity resources.

Human and relational enablers showed mid-to-high average values, with greater dispersion than the core technical indicators. Cybersecurity awareness (CSA) items were above the midpoint (CSA1: "Our organization provides employees with effective cybersecurity knowledge and understanding", M = 5.382; SD = 1.439; CSA2: "Our organization fosters a strong cybersecurity culture and employee engagement", M = 5.200; SD = 1.494; CSA3: "Our organization's employees demonstrate awareness of cybersecurity threats and best practices in their daily work", M = 5.153; SD = 1.337), suggesting generally positive assessments of awareness-related culture and practices. Cybersecurity training (CST) was rated slightly lower than awareness, with the lowest means within this block observed for specialized technical training (CST2: "Our organization provides effective cybersecurity skill development and competency building", M = 4.876; SD = 1.496) and comprehensive training effectiveness measurement (CST3: "Our organization's cybersecurity training program is continuously improved based on formal assessments", M = 4.941; SD = 1.549). Alliance and collaboration (CSAC) displayed relatively lower means and among the highest dispersions, indicating that collaborative posture and intelligence-sharing were uneven across organizations (CSAC1: "Our organization demonstrates effective cybersecurity partnerships and development", M = 5.071; SD = 1.490; CSAC2: "Our organization exhibits effective cybersecurity information sharing and intelligence collaboration", M = 4.924; SD = 1.569; CSAC3: "Our organization participates actively in industry-wide cybersecurity initiatives", M = 4.659; SD = 1.741). The particularly high dispersion of CSAC3 suggests that threat- or insight-sharing practices vary widely across industries, regulatory frameworks, and ecosystem integration.

Governance-related constructs had a similar variation in management attention. The cybersecurity top management support (CSTMS) demonstrated mid-range means with relatively high dispersion (CSTMS1: "Our organization’s top management demonstrates a strong commitment to cybersecurity and effective resource allocation", M = 5.006; SD = 1.673; CSTMS2: "Our organization’s leadership exhibits effective cybersecurity governance structure and CISO positioning", M = 4.976; SD = 1.602; CSTMS3: "Our organization's top management ensures accountability for cybersecurity performance", M = 4.953; SD = 1.663). Cybersecurity top management risk perception (CSTMRP) was slightly lower on average and similarly dispersed (CSTMRP1: "Our organization's top management demonstrates accurate

understanding of cybersecurity risk assessment", M = 4.829; SD = 1.744; CSTMRP2: "Our organization's senior leadership exhibits effective cybersecurity threat awareness and intelligence utilization", M = 4.871; SD = 1.564; CSTMRP3: "Our organization's executives make decisions with comprehensive awareness of cyber risks", M = 4.882; SD = 1.617). This pattern indicates that, although many organizations report strong technical foundations, the perceived intensity and consistency of senior leadership's risk awareness and support vary substantially, with consequential implications for the governance pathways specified in the model.

Finally, the environmental dynamism indicators were closest to the midpoint of the scale and exhibited relatively high dispersion, suggesting heterogeneous external conditions across respondents. Market turbulences (MT) were reported at moderate levels (MT1: "Our organization operates in an unpredictable and rapidly changing market environment", M = 4.776; SD = 1.712; MT2: "Our organization faces frequent and intense competitive threats and market disruptions", M = 4.588; SD = 1.701; MT3: "Our organization experiences external stakeholder pressure and conflicting demands (e.g. from regulators vs. customers)", M = 4.676; SD = 1.729). Technological turbulences (TT) were similar, with TT2 somewhat higher than TT1 and TT3 (TT1: "Our organization operates in a rapidly evolving and unpredictable technological environment", M = 4.647; SD = 1.694; TT2: "Our organization experiences complexity in integrating and managing multiple emerging technologies", M = 5.000; SD = 1.484; TT3: "Our organization encounters pressure to adopt new technologies to remain competitive rapidly", M = 4.706; SD = 1.681). The combination of moderate means and sizable dispersion for MT and TT suggests that contextual pressures differ meaningfully across organizations, supporting their role as environmental conditions in the subsequent structural analysis.

Table 19 summarizes the distribution of the construct-level averages (row-wise means of the corresponding manifest items). Overall, the average scores exceed the midpoint of the seven-point scale for the core capability and internal enabler constructs, with the highest means observed for technological infrastructure (TI_avg: M = 5.514; SD = 1.120) and cybersecurity risk maturity (CSRM_avg: M = 5.473; SD = 1.188). Organizational resilience (R_avg) is similarly high (M = 5.296; SD = 1.235), consistent with the expectation that greater maturity and infrastructure are associated with stronger perceived resilience.

The human- and capability-related constructs show slightly lower but still favorable levels: cybersecurity resources and capabilities (CSRC_avg: M = 5.316; SD = 1.346), cybersecurity awareness (CSA_avg: M = 5.245; SD = 1.253), and cybersecurity training (CST_avg: M = 4.988; SD = 1.319). Relational and governance constructs are comparatively weaker and more heterogeneous, with cybersecurity alliance and collaboration (CSAC_avg: M = 4.884; SD = 1.414) and both management-related averages showing mid-range means and the largest dispersion (CSTMS_avg: M = 4.978; SD = 1.539; CSTMRP_avg: M = 4.861; SD = 1.538). This indicates that collaboration intensity and senior management attention vary substantially across organizations and may represent differentiating factors in the model. Finally, the contextual conditions—market turbulence (MT_avg: M = 4.680; SD = 1.393) and technological turbulence (TT_avg: M = 4.784; SD = 1.320)—are near the midpoint, with notable variability, suggesting that organizations operate under varying levels of external dynamism.

Table 19: Descriptive statistics for average of manifest variables

Variable	Valid	Mean	Std. Deviation	Minimum	Maximum
R_avg	170	5.296	1.235	1.000	7.000
CSRM_avg	170	5.473	1.188	1.000	7.000
TI_avg	170	5.514	1.120	1.000	7.000
CSRC_avg	170	5.316	1.346	1.000	7.000
CSA_avg	170	5.245	1.253	1.000	7.000
CST_avg	170	4.988	1.319	1.000	7.000
CSAC_avg	170	4.884	1.414	1.000	7.000
CSTMS_avg	170	4.978	1.539	1.000	7.000
CSTMRP_avg	170	4.861	1.538	1.000	7.000
MT_avg	170	4.680	1.393	1.000	7.000
TT_avg	170	4.784	1.320	1.000	7.000

Source: Author's work

Across the surveyed large Swiss enterprises, respondents generally rated their organizations above the midpoint on core cyber capabilities, particularly technological infrastructure and cybersecurity risk maturity, suggesting a comparatively strong technical baseline. In contrast, the most uneven areas were collaboration and intelligence sharing with external partners, as well as top management's perception of risk and support, which varied substantially across organizations. For practitioners, this pattern implies that incremental gains in resilience are likely to come less from additional technology alone and more from strengthening governance (clear executive ownership, consistent risk attention) and institutionalizing external collaboration (structured information sharing, third-party coordination, and joint response practices), especially under differing levels of market and technological turbulence.

5.2.4. Measurement model

Table 20 reports Pearson correlations among construct-level averages (means of the manifest indicators for each construct). As a preliminary diagnostic, such a matrix is typically used to (i) check whether the empirical associations align with the theorized nomological network and (ii) flag potential risks for the subsequent confirmatory measurement model (for example, redundancy between constructs or excessive overlap that could compromise discriminant validity). This sequencing is consistent with established recommendations to examine bivariate relations descriptively before moving to confirmatory factor analysis and full structural equation modeling (Anderson & Gerbing, 1988; Brown, 2015; Kline, 2016).

Substantively, the correlation pattern is coherent and strongly integrated among the internal cyber capability constructs. Resilience (R_avg) correlates strongly with cybersecurity risk maturity (CSRM_avg; r = 0.775), technological infrastructure (TI_avg; r = 0.750), resources and capabilities (CSRC_avg; r = 0.741), awareness (CSA_avg; r = 0.729), training (CST_avg; r = 0.732), alliance and collaboration (CSAC_avg; r = 0.684), and top management support (CSTMS_avg; r = 0.712). These magnitudes fall within the “large” range by conventional benchmarks and indicate that the constructs covary in the expected direction for a capability-building logic (Cohen, 1988). In methodological terms, this is an encouraging sign for convergent coherence at the nomological level: constructs that should be positively related are, in fact, strongly and consistently related.

At the same time, several coefficients are sufficiently high to warrant explicit scrutiny in the confirmatory phase. In particular, CSTMS_avg and top management risk perception (CSTMRP_avg) correlate at r = 0.847, and awareness (CSA_avg) with training (CST_avg) at r

= 0.822. Such magnitudes can reflect a theoretically meaningful tight coupling, but they may also signal limited discriminant validity or conceptual redundancy (i.e., indicators may be capturing a very similar underlying construct). This is precisely why correlation matrices should not be treated as evidence of discriminant validity on their own; instead, discriminant validity will be evaluated in the next steps within the measurement model using confirmatory techniques (for example, factor correlations with confidence intervals, Fornell–Larcker-style comparisons, or related diagnostics), and by inspecting whether constructs remain empirically distinct once measurement error is modelled (Brown, 2015; Fornell & Larcker, 1981; Kline, 2016).

Environmental turbulence constructs exhibit weak-to-moderate associations with the internal capability block, consistent with the view that turbulence is an exogenous contextual factor rather than an internal capability dimension. Market turbulence (MT_avg) correlates modestly with most cyber capability constructs ($r \approx 0.35–0.48$), and technological turbulence (TT_avg) shows a similar pattern ($r \approx 0.35–0.49$). The correlation between MT_avg and TT_avg is high ($r = 0.778$), suggesting that respondents may perceive these turbulence dimensions as closely linked. Methodologically, this does not, again, invalidate the model. However, it implies that (i) the theoretical boundary between the two turbulence constructs should be clearly articulated, and (ii) confirmatory testing should verify whether a two-factor representation fits better than a more parsimonious alternative (for example, a higher-order "turbulence" factor), using established model comparison logic (Brown, 2015; Kline, 2016).

Finally, it is important to interpret these correlations as descriptive *rather than confirmatory* evidence. Because the coefficients are computed on construct averages, they do not account for measurement error and can either inflate or obscure relationships relative to latent-variable correlations estimated in CFA/SEM (Bollen, 1989; Kline, 2016). Accordingly, Table 20 is best framed as an initial coherence check that supports progression to the confirmatory assessment, in which the measurement model will determine whether the strong inter-construct associations reflect theoretically appropriate integration rather than insufficient empirical distinctiveness (Anderson & Gerbing, 1988; Brown, 2015).

Table 20: Pearson correlation coefficients of the average of manifest variables

Variable	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.
1. R_avg	—										
2. CSRM_avg	0.775	—									
3. TI_avg	0.750	0.708	—								
4. CSRC_avg	0.741	0.730	0.731	—							
5. CSA_avg	0.729	0.624	0.682	0.738	—						
6. CST_avg	0.732	0.662	0.658	0.714	0.822	—					
7. CSAC_avg	0.684	0.643	0.602	0.667	0.675	0.739	—				
8. CSTMS_avg	0.712	0.641	0.590	0.691	0.747	0.751	0.689	—			
9. CSTMRP_avg	0.759	0.660	0.651	0.686	0.730	0.742	0.744	0.847	—		
10. MT_avg	0.374	0.352	0.437	0.35	0.410	0.403	0.482	0.404	0.47	—	
11. TT_avg	0.399	0.354	0.413	0.379	0.365	0.362	0.487	0.394	0.462	0.778	—

Source: Author's work

Note: All coefficients are statistically significant at 1%; Source: Author's work

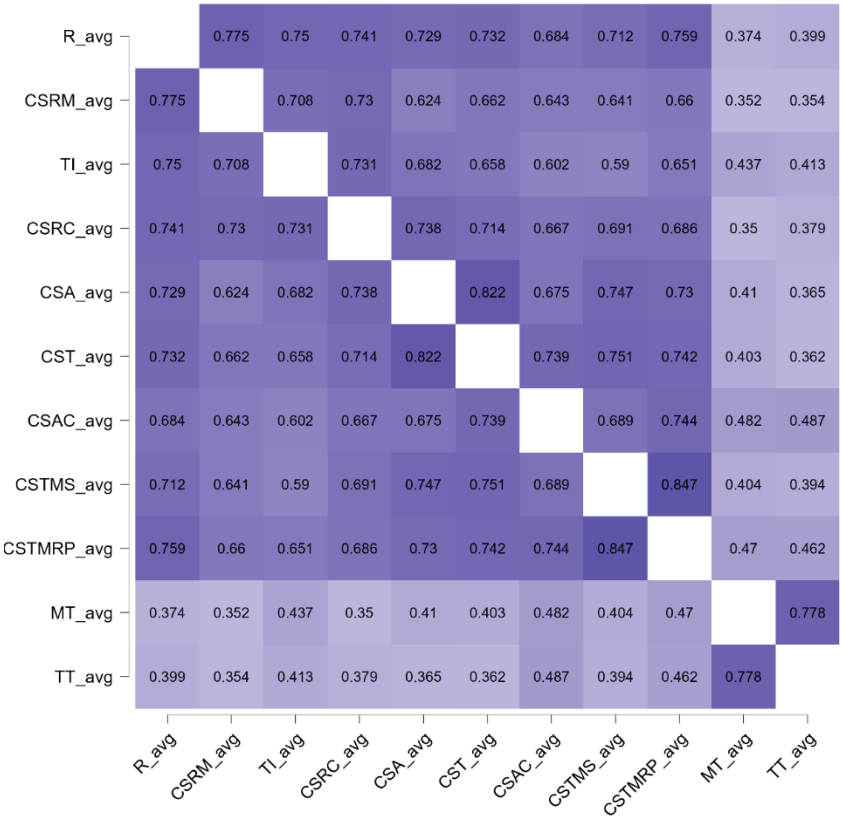


Figure 3: Pearson's r heatmap

Source: Author's work

Table 21 presents the chi-square statistics for the baseline (independence) model and the specified factor model, both estimated using maximum likelihood. The chi-square for the factor model is statistically significant (X^2 = 659.769, df = 379, p < .001). In confirmatory factor analysis, the chi-square test is often statistically significant in models of moderate complexity because it is highly sensitive to sample size and small departures from exact fit. For this reason, the chi-square statistic is typically interpreted as a general diagnostic and considered alongside approximate fit indices when evaluating overall model fit (Kline, 2016). Relative to the baseline model (X^2 = 4,963.040, df = 465), the factor model yields a substantially lower chi-square value, indicating that the specified measurement structure reproduces the observed covariance matrix more closely than the independence model.

Table 21: Chi-square test

Model	X^2	df	p
Baseline model	4,963.040	465	
Factor model	659.769	379	< .001

Source: Author's work; Note. The estimator is ML. The test statistic is standard. The standard error method is standard.

Table 22 summarizes the approximate fit indices for the confirmatory factor model. The comparative fit index (CFI = 0.938) and Tucker–Lewis index (TLI = 0.923) indicate adequate incremental fit relative to the baseline model, as these values are consistent with conventional benchmarks for acceptable fit in structural equation modeling practice (Bentler, 1990; Kline, 2016). The root mean square error of approximation (RMSEA = 0.066; 90% confidence interval: 0.058–0.074) suggests a reasonable level of approximation error, with the interval indicating that plausible population misfit is unlikely to be severe (Browne & Cudeck, 1993; Kline, 2016). The standardized root mean square residual (SRMR = 0.044) is low, supporting good fit in terms of standardized residuals and indicating that the model reproduces the observed associations with relatively small average discrepancies (Hu & Bentler, 1999).

The RMSEA p-value (0.001) indicates that the hypothesis of "close fit" (often framed as RMSEA ≤ 0.05) is not supported. This result is not uncommon and should be interpreted in conjunction with the RMSEA point estimate and confidence interval; taken together, these statistics support an overall conclusion of acceptable model fit rather than exact or "close" fit (Browne & Cudeck, 1993; Kline, 2016).

Table 22: Fit indices

Fit indices	Value
Comparative Fit Index (CFI)	0.938
Tucker-Lewis Index (TLI)	0.923
Root mean square error of approximation (RMSEA)	0.066

RMSEA 90% CI lower bound	0.058
RMSEA 90% CI upper bound	0.074
RMSEA p-value	0.001
Standardized root mean square residual (SRMR)	0.044

Source: Author's work

Table 23 shows that all standardized factor loadings are positive, substantial, and statistically significant at the 1% level, supporting convergent validity at the indicator level. Most loadings are in the moderate-to-high range (approximately 0.67–0.94), and the associated R^2 values indicate that the latent constructs explain a meaningful share of indicator variance. Particularly strong measurement is observed for selected indicators such as CSRM2 ($\lambda = 0.912$; $R^2 = 0.831$), CSRC2 ($\lambda = 0.925$; $R^2 = 0.855$), CSTMS2 ($\lambda = 0.936$; $R^2 = 0.876$), and the CSTMRP indicators ($\lambda \approx 0.893$–0.919; $R^2 \approx 0.797$–0.845). In contrast, environmental turbulence indicators show comparatively lower explained variance (e.g., MT1: $R^2 = 0.486$; TT2: $R^2 = 0.454$), consistent with these constructs being more context-dependent and potentially more heterogeneous across organizations.

Two measurement blocks were refined more substantially. For Market Turbulence (MT), only MT1 ("Our organization operates in an unpredictable and rapidly changing market environment") and MT2 ("Our organization faces frequent and intense competitive threats and market disruptions") were retained, while MT3 ("Our organization experiences external stakeholder pressure and conflicting demands") was removed because it did not load acceptably on the intended factor; the resulting two item specification is acknowledged as a limitation. The retained items show acceptable-to-strong loadings (0.697 and 0.834) and unpredictability and threat intensity of the market environment; however, the reduced two-item specification indicates that the "stakeholder pressure" facet did not align sufficiently with the underlying turbulence factor in this sample and should be interpreted as a narrower operationalization of market turbulence focused on market unpredictability and competitive threats.

Similarly, for Technological Turbulence (TT), only TT2 ("Our organization experiences complexity in integrating and managing multiple emerging technologies") and TT3 ("Our organization encounters pressure to adopt new technologies to remain competitive rapidly")

were retained. In contrast, TT1 ("Our organization operates in a rapidly evolving and unpredictable technological environment") was removed for the same reason. The loadings for the retained indicators are 0.674 and 0.820, suggesting that respondents differentiated turbulence primarily by integration complexity and adoption pressure rather than by general environmental unpredictability. As with MT, the resulting TT construct represents a more specific conceptual slice of technological turbulence (integration and adoption challenges) rather than a broader environmental interpretation.

Taken together, the factor-loading results indicate that the measurement model performs robustly for the core cybersecurity and governance constructs. In contrast, the environmental context constructs (market turbulence and technological turbulence) require item reduction to attain acceptable psychometric properties. Accordingly, structural-path interpretations involving market turbulence and technological turbulence should be made with the explicit caveat that these latent variables operationalize the retained facets of turbulence (market unpredictability and competitive-threat intensity for market turbulence; integration complexity and adoption pressure for technological turbulence) rather than the full conceptual breadth implied by the original three-item scales, consistent with standard guidance on interpreting refined confirmatory factor analysis measures and their implications for construct validity and substantive inference (Brown, 2015; Kline, 2016).

Table 23: Factor loadings and coefficients of determination

Factor	Indicator	Std. estimate	Std. Error	z-value	R^2
R	R1	0.784	0.033	23.803***	0.615
	R2	0.853	0.025	33.687***	0.727
	R3	0.786	0.033	24.027***	0.618
CSRM	CSRM1	0.787	0.033	23.636***	0.619
	CSRM2	0.912	0.02	45.373***	0.831
	CSRM3	0.793	0.033	24.368***	0.629
TI	TI1	0.795	0.033	23.837***	0.632

	TI2	0.737	0.04	18.624***	0.543
	TI3	0.818	0.031	26.504***	0.67
CSRC	CSRC1	0.777	0.034	23.046***	0.604
	CSRC2	0.925	0.018	52.067***	0.855
	CSRC3	0.797	0.031	25.353***	0.635
CSA	CSA1	0.795	0.032	25.107***	0.633
	CSA2	0.877	0.023	38.699***	0.769
	CSA3	0.767	0.035	21.934***	0.588
CST	CST1	0.816	0.029	27.801***	0.665
	CST2	0.855	0.025	34.452***	0.732
	CST3	0.817	0.029	27.938***	0.667
CSAC	CSAC1	0.82	0.03	27.272***	0.672
	CSAC2	0.897	0.022	40.438***	0.805
	CSAC3	0.757	0.037	20.408***	0.573
CSTMS	CSTMS1	0.856	0.023	37.469***	0.734
	CSTMS2	0.936	0.013	70.979***	0.876
	CSTMS3	0.91	0.016	56.289***	0.828
CSTMRP	CSTMRP1	0.919	0.015	61.082***	0.845
	CSTMRP2	0.898	0.018	50.797***	0.806
	CSTMRP3	0.893	0.018	48.849***	0.797
MT	MT1	0.697	0.049	14.129***	0.486
	MT2	0.834	0.043	19.602***	0.696
TT	TT3	0.82	0.05	16.525***	0.673

	TT2	0.674	0.055	12.324***	0.454

Note: *** statistically significant at 1%; Source: Author's work

Table 24 provides further support for measurement quality, including convergent validity and internal consistency. All constructs meet the conventional AVE criterion (AVE > 0.50), indicating that each latent construct explains, on average, more than half of the variance in its indicators and thereby supporting convergent validity (Fornell & Larcker, 1981). Reliability estimates are generally strong at the construct level: coefficient omega and Cronbach's alpha exceed 0.80 for the central internal capability and governance constructs, with particularly high values for top management support and top management risk perception, consistent with high internal consistency of their indicator sets (Cronbach, 1951; McDonald, 1999). The turbulence constructs exhibit comparatively lower yet acceptable reliability (MT: ω = 0.741; TT: ω = 0.727), which is plausible given more context-sensitive and potentially heterogeneous environmental perceptions. Finally, the "Total" reliability values are extremely high; however, such instrument-level indices are typically less diagnostic in multi-construct instruments because they can largely reflect aggregation across correlated dimensions rather than reliability of any specific construct. Accordingly, construct-level reliability remains the more appropriate basis for evaluating measurement quality in the present model (Kline, 2016).

Table 24: Average variance extracted and reliability indicators

Factor	AVE	Coefficient ω	Coefficient α
R	0.652	0.852	0.846
CSRM	0.685	0.866	0.867
TI	0.622	0.828	0.822
CSRC	0.698	0.861	0.859
CSA	0.669	0.857	0.853
CST	0.688	0.868	0.868
CSAC	0.676	0.865	0.857

CSTMS	0.811	0.928	0.928
CSTMRP	0.818	0.93	0.929
MT	0.59	0.741	0.735
TT	0.577	0.727	0.709
Total		0.974	0.97

Source: Author's work

Table 25 presents the heterotrait–monotrait (HTMT) ratios used to assess discriminant validity between the latent constructs. The results indicate that discriminant validity is generally supported across the measurement model, particularly for the environmental turbulence constructs (MT and TT) relative to the internal organizational constructs. However, three construct pairs show HTMT values that are close to, or exceed, conservative thresholds: cybersecurity awareness and cybersecurity training (CSA–CST = 0.956), top management support and top management risk perception (CSTMS–CSTMRP = 0.908), and resilience and cybersecurity risk maturity (R–CSRM = 0.903). These elevated ratios imply that these pairs are empirically very closely related in the sample and only partially distinguishable as separate constructs (Henseler et al., 2014; Kline, 2016; Brown, 2015). Substantively, this is consistent with organizational practice: awareness and training are typically implemented as an integrated capability; managerial risk perception is strongly aligned with managerial support; and resilience is closely linked to mature cyber risk management. In the context of this study, the measurement model therefore captures a set of tightly connected yet theoretically meaningful dimensions, with the strongest overlap occurring among the most proximate "human capability" and "governance" constructs, and between maturity and resilience.

Table 25: Heterotrait-monotrait ratio

Factor	R	CSRM	TI	CSRC	CSA	CSAC	CSTMS	CSTMRP	MT	TT	CST
R	1.000										

CSRM	0.903	1.000									
TI	0.897	0.829	1.000								
CSRC	0.865	0.841	0.854	1.000							
CSA	0.857	0.726	0.811	0.853	1.000						
CSAC	0.802	0.745	0.709	0.768	0.782	1.000					
CSTMS	0.799	0.712	0.67	0.763	0.834	0.773	1.000				
CSTMRP	0.854	0.735	0.741	0.761	0.818	0.832	0.908	1.000			
MT	0.508	0.48	0.601	0.475	0.605	0.634	0.526	0.586	1.000		
TT	0.426	0.403	0.414	0.407	0.39	0.497	0.448	0.474	0.789	1.000	
CST	0.856	0.765	0.778	0.823	0.956	0.858	0.839	0.829	0.562	0.417	1.000

Source: Author's work

Overall, the results of the measurement model assessment indicate that the questionnaire operationalized the study constructs with satisfactory psychometric quality and provides an adequate basis for testing the proposed research model. The construct-level correlations (Table 20) are consistent with the theoretical logic of a tightly connected cyber capability system: cybersecurity risk maturity, internal resources and infrastructure, human capability (awareness and training), collaboration, and top-management governance move together strongly and in

the expected direction, whereas market turbulence and technological turbulence show weaker-to-moderate relationships with the internal constructs and a strong association with each other. This pattern supports the conceptual separation between internal organizational capabilities and external environmental dynamism, while also highlighting that several internal constructs are empirically very close to one another.

The confirmatory factor analysis results further support the measurement structure. Although the chi-square test for the factor model is statistically significant (Table 21), the global fit indices (Table 22) indicate acceptable-to-good approximate model fit (CFI = 0.938; TLI = 0.923; RMSEA = 0.066; SRMR = 0.044), which is appropriate for a multi-construct model of this complexity and sample size. At the indicator level, all retained items show positive, substantial, and statistically significant standardized loadings (Table 23), with many indicators demonstrating strong explained variance (R^2). Convergent validity and internal consistency are supported by AVE values exceeding 0.50 for all constructs and by generally high reliability coefficients (Table 24), particularly for the governance-related constructs.

A critical implication concerns the distinctiveness of constructs across conceptually adjacent domains. HTMT ratios (Table 25) indicate that discriminant validity is generally satisfactory, especially for the environmental turbulence constructs relative to the internal capability constructs; however, three pairs exhibit very high overlap (CSA–CST, CSTMS–CSTMRP, and R–CSRM). Substantively, this suggests that respondents in large enterprises tend to view awareness and training as an integrated practice set, perceive risk and top management support as tightly coupled aspects of governance, and view cybersecurity risk maturity as closely intertwined with resilience outcomes. In practical terms, these findings do not undermine the measurement model; however, they indicate that certain aspects of the model reflect highly interdependent organizational capabilities. Therefore, the interpretation of structural effects among the most proximate constructs should recognize that estimated paths may reflect incremental effects beyond substantial shared variance.

Finally, the refinement of the turbulence constructs is noteworthy. Item reduction in MT and TT (Table 23) indicates that, in this sample, environmental turbulence was captured more reliably through market unpredictability/competitive threats and integration/adoption challenges than through external stakeholder pressure or general technological unpredictability. Consequently, MT and TT should be interpreted as narrower operationalizations of environmental turbulence in the subsequent structural analysis.

Given the acceptable model fit, strong indicator loadings, and satisfactory reliability and convergent validity, together with a transparent acknowledgment of high construct proximity in specific pairs, the measurement model supports progression to structural equation modeling. The next section, therefore, estimates the structural paths specified by hypotheses H1–H10, evaluates their magnitudes and statistical significance, and assesses how governance, internal cyber capabilities, and environmental turbulence jointly explain cybersecurity risk maturity and organizational resilience in the surveyed large Swiss enterprises.

5.2.5. Structural equations modeling

Table 26 reports global fit information for the estimated structural equation model (Model 1) based on maximum likelihood estimation. The baseline chi-square test is statistically significant ($\chi^2 = 833.981$, df = 420, $p < .001$), as expected in SEM with a moderate sample size and a non-trivial number of free parameters (76), given that the chi-square test is highly sensitive to even small departures from exact fit. Therefore, the chi-square result is interpreted as an indicator of imperfect exact fit rather than as evidence that the model is unusable.

Table 26: SEM model fit

Model fit	n	n(Parameters)		Baseline test		
		Total	Free	χ^2	df	p
Model 1	170	76	76	833.981	420.000	< .001

Note. Estimator is ML. The model test is standard. An information matrix is expected. Standard errors are standard.; Source: Author's work

Table 27 indicates that the structural model achieved an overall level of fit that is acceptable for hypothesis testing, albeit not a "close fit" by the most stringent criteria. The comparative fit index (CFI = 0.908) meets the commonly used benchmark of approximately 0.90 for acceptable fit (Bentler, 1990; Kline, 2016), while the Tucker–Lewis index (TLI = 0.898) is marginally below this conventional threshold and therefore suggests some remaining model misspecification or complexity relative to the achieved fit (Kline, 2016). The root mean square error of approximation is RMSEA = 0.076 (90% CI: 0.069–0.084), which falls within the range often interpreted as "reasonable" or "acceptable" approximation error (Browne & Cudeck,

1993), rather than the stricter "close fit" criterion (RMSEA ≤ 0.05) applied to the measurement model (Browne & Cudeck, 1993). The standardized root mean square residual (SRMR = 0.062) is below the frequently cited 0.08 cutoff, supporting acceptable residual-based fit (Hu & Bentler, 1999). Taken together, the indices suggest that the SEM provides a workable representation of the observed covariance structure for evaluating the proposed structural relationships. At the same time, the slightly elevated RMSEA and borderline TLI indicate that the model fit should be interpreted as adequate rather than excellent.

Table 27: Fit indices of SEM model

Fit indices	Value
Comparative Fit Index (CFI)	0.908
Tucker-Lewis Index (TLI)	0.898
Root mean square error of approximation (RMSEA)	0.076
RMSEA 90% CI lower bound	0.069
RMSEA 90% CI upper bound	0.084
RMSEA p-value	0
Standardized root mean square residual (SRMR)	0.062

Source: Author's work

Table 28 summarizes the standardized factor loadings for the SEM measurement component and indicates generally strong indicator reliability and convergent measurement. All loadings are positive and statistically significant ($p < .001$), with standardized estimates ranging from 0.657 to 0.929, and most indicators exceeding the commonly used 0.70 guideline for well-performing items, indicating satisfactory indicator reliability (Black & Babin, 2019; Kline, 2016). The strongest measurement is observed for the governance constructs, particularly cybersecurity top management risk perception (CSTMRP; 0.895–0.919) and top management support (CSTMS; 0.849–0.929), with R^2 values (0.721–0.863) indicating that the latent constructs account for a substantial share of the variance in their indicators. The core capability constructs (CSRM, TI, CSRC, CSA, CST, CSAC, and R) also exhibit consistently high loadings

(typically 0.75–0.89), supporting the instrument's adequacy for modeling relationships among cyber maturity, enabling capabilities, and resilience. Two indicators are comparatively weaker but still acceptable in context: MT1 (0.657; $R^2 = 0.432$) and CSAC3 (0.686; $R^2 = 0.470$). These "borderline" values suggest more heterogeneous respondent interpretations or greater measurement error for these specific facets (market dynamism and insights sharing). However, they still contribute substantively to content coverage and remain clearly related to their intended constructs. Overall, the pattern of strong and significant loadings supports proceeding to the structural (hypothesis-testing) part of the SEM, while recognizing that the environmental turbulence indicators (MT, TT) exhibit relatively lower explained variance than the internal organizational capability constructs, consistent with the more context-dependent nature of these conditions.

Table 28: Factor loadings of the SEM model

Latent	Indicator		Std. estimate	Std. error	z-value	p	R^2
CSA	CSA1	lambda_5_1	0.794	0.033	24.341	< .001	0.63
	CSA2	lambda_5_2	0.888	0.023	39.421	< .001	0.789
	CSA3	lambda_5_3	0.758	0.037	20.724	< .001	0.575
CSAC	CSAC1	lambda_6_1	0.768	0.034	22.732	< .001	0.589
	CSAC2	lambda_6_2	0.804	0.029	27.331	< .001	0.647
	CSAC3	lambda_6_3	0.686	0.043	16.031	< .001	0.47
CSRC	CSRC1	lambda_4_1	0.796	0.033	24.367	< .001	0.634
	CSRC2	lambda_4_2	0.877	0.024	36.734	< .001	0.769
	CSRC3	lambda_4_3	0.828	0.029	28.387	< .001	0.685
CSRM	CSRM1	lambda_2_1	0.759	0.035	21.413	< .001	0.577
	CSRM2	lambda_2_2	0.877	0.022	40.760	< .001	0.769
	CSRM3	lambda_2_3	0.767	0.035	22.165	< .001	0.588

CST	CST1	lambda_11_1	0.805	0.031	26.213	< .001	0.648
	CST2	lambda_11_2	0.859	0.025	34.999	< .001	0.738
	CST3	lambda_11_3	0.817	0.029	27.952	< .001	0.668
CSTMRP	CSTMRP1	lambda_8_1	0.919	0.015	59.774	< .001	0.844
	CSTMRP2	lambda_8_2	0.895	0.018	49.075	< .001	0.801
	CSTMRP3	lambda_8_3	0.895	0.018	48.988	< .001	0.8
CSTMS	CSTMS1	lambda_7_1	0.849	0.024	35.987	< .001	0.721
	CSTMS2	lambda_7_2	0.929	0.014	68.569	< .001	0.863
	CSTMS3	lambda_7_3	0.905	0.016	55.000	< .001	0.819
MT	MT1	lambda_9_1	0.657	0.053	12.288	< .001	0.432
	MT2	lambda_9_2	0.877	0.041	21.271	< .001	0.77
R	R1	lambda_1_1	0.785	0.034	23.285	< .001	0.617
	R2	lambda_1_2	0.835	0.028	29.514	< .001	0.698
	R3	lambda_1_3	0.794	0.033	24.269	< .001	0.631
TI	TI1	lambda_3_1	0.794	0.035	22.490	< .001	0.63
	TI2	lambda_3_2	0.759	0.039	19.508	< .001	0.576
	TI3	lambda_3_3	0.796	0.035	22.717	< .001	0.634
TT	TT3	lambda_10_1	0.770	0.051	15.068	< .001	0.594
	TT2	lambda_10_2	0.718	0.053	13.554	< .001	0.516

Source: Author's work

Table 29 summarizes convergent validity and internal consistency for the latent constructs in the structural equation model. Average variance extracted values exceed the commonly applied 0.50 criterion for all constructs (range: 0.555–0.815), indicating that each construct explains more than half of the variance in its indicators, thereby supporting convergent validity (Fornell

& Larcker, 1981). Reliability is also satisfactory: Cronbach's alpha is at or above 0.71 for all constructs and particularly high for the governance-related constructs (CSTMS: α = 0.928; CSTMRP: α = 0.930), consistent with their strong and homogeneous indicator sets. Coefficient omega likewise indicates acceptable-to-strong composite reliability across constructs (ω = 0.713–0.928) (Black & Babin, 2019). The comparatively lower omega for CSAC (ω = 0.724), while still acceptable, suggests somewhat greater heterogeneity among its indicators relative to the other cyber capability constructs and should be considered when interpreting effects involving collaboration/alliance (Black & Babin, 2019). Finally, although the "Total" reliability coefficients are very high (α = 0.970; ω = 0.944), such global indices are less diagnostically informative in a multi-construct instrument and should be interpreted with caution (Fornell & Larcker, 1981; Black & Babin, 2019).

Table 29: Average variance extracted and reliability indicators of the SEM model

Latent	AVE	Coefficient α	Coefficient ω
R	0.642	0.847	0.838
CSRM	0.637	0.87	0.8
TI	0.614	0.828	0.824
CSRC	0.696	0.87	0.875
CSA	0.665	0.853	0.856
CST	0.684	0.867	0.865
CSAC	0.569	0.861	0.724
CSTMS	0.801	0.928	0.915
CSTMRP	0.815	0.93	0.928
MT	0.601	0.735	0.744
TT	0.555	0.712	0.713
Total		0.97	0.944

Source: Author's work

Table 30 reports the standardized structural coefficients from the estimated structural equation model, providing clear empirical validation of the research model's proposed cascading logic (Figure 1). Overall, the model operates as a tightly coupled capability system in which governance-related drivers shape collaboration, collaboration strengthens internal capabilities, internal capabilities build cybersecurity risk maturity, and maturity translates into organizational resilience. The high explained variance for most endogenous constructs (R^2 ranging from 0.319 to 0.934, and from 0.702 to 0.934 in the central parts of the model) indicates that the specified determinants account for a substantial proportion of the variance in the focal constructs and that the nomological structure is strongly supported among surveyed large Swiss enterprises.

At the outcome level, cybersecurity risk maturity has a very strong positive effect on organizational resilience ($\beta = 0.967$, $p < .001$; $R^2(R) = 0.934$), supporting H1. This result is consistent with the theoretical framing that mature cyber risk management institutionalizes identification, mitigation, and continuous improvement processes that enhance an organization's ability to withstand, recover from, and adapt to cyber disruption (Linkov & Kott, 2018; Rajan et al., 2021). Substantively, the magnitude of this coefficient suggests that, within this sample, resilience is largely expressed through the maturity of cyber risk governance and lifecycle practices, rather than being driven directly by exogenous turbulence or other antecedents.

Cybersecurity risk maturity, in turn, is significantly driven by internal capability block. Technological infrastructure positively predicts cybersecurity risk maturity ($\beta = 0.477$, $p < .001$), supporting H2a. This reinforces the notion that consistent and integrated infrastructure enables continuous monitoring, detection, and control—core requirements for a transition from ad hoc to systematic risk management (Van Laak, 2004; Subashini & Kavitha, 2011; Almuhammadi & Alsaleh, 2017). Resources and capabilities for cybersecurity are also positively impactful ($\beta = 0.376$, $p < .001$), reinforcing H2b, consistent with the assumption that resourcing, specialized teams, and formalized processes enhance the entity's capacity to carry out coherent, repeatable risk identification and mitigation throughout the cyber risk lifecycle (Rajan et al., 2021; Landoll, 2021; Kosub, 2015). Together, these results support the thesis that maturity is primarily built on tangible technological and organizational capabilities.

The human-capability mechanisms show a more nuanced pattern. Cybersecurity training is positively associated with cybersecurity risk maturity ($\beta = 0.336$), which is only marginally

significant at the 10% level ($p = 0.052$), providing weaker support for H3b. By contrast, cybersecurity awareness is not statistically significant and has a negative sign ($\beta = -0.200$, $p = 0.202$), leading to rejection of H3a. Interpreted in light of the earlier measurement results, this pattern is plausible: awareness and training were empirically very proximate (high HTMT), and both were strongly driven by collaboration, leaving limited residual variance for awareness to explain maturity once training and other capability variables are included. Substantively, this configuration suggests that "awareness" may operate more as a general cultural condition correlated with other enablers, whereas structured training may be the more directly actionable human-capability mechanism that translates into routinised practices supporting maturity (Li et al., 2019; Trim & Upton, 2013; Moustafa et al., 2021; Cains et al., 2022). The results, therefore, support a cautious interpretation: human capability is relevant, but its contribution appears to flow primarily through structured training and through upstream collaboration channels, rather than through awareness as a separable predictor.

The collaboration block behaves exactly as hypothesized and serves as a powerful amplifier of upstream capabilities. Cybersecurity alliance and collaboration strongly predict technological infrastructure ($\beta = 0.838$, $p < .001$; $R^2(TI) = 0.702$) and cybersecurity resources and capabilities ($\beta = 0.879$, $p < .001$; $R^2(CSRC) = 0.773$), supporting H4a and H4b. It also strongly predicts cybersecurity awareness ($\beta = 0.938$, $p < .001$; $R^2(CSA) = 0.880$) and cybersecurity training ($\beta = 0.959$, $p < .001$; $R^2(CST) = 0.920$), supporting H5a and H5b. These effects are consistent with the logic advanced in the research model: structured collaboration and information-sharing arrangements provide early threat visibility, shared practices, pooled expertise, and joint learning loops that strengthen internal technical roadmaps, capability development, and workforce learning processes (Fransen et al., 2015; Trim & Upton, 2013). Empirically, the large coefficients indicate that collaboration is not merely a peripheral enabler; it appears to be a central integrator that simultaneously develops multiple internal capability dimensions.

Governance relationships are also strongly supported and demonstrate the expected cascading leadership mechanism. Top management risk perception strongly predicts top management support ($\beta = 0.933$, $p < .001$; $R^2(CSTMS) = 0.870$), supporting H7 and aligning with the theoretical claim that perceived strategic salience of cyber risk mobilizes executive attention, resourcing, and sponsorship of security initiatives (Cebula et al., 2014; Rothrock et al., 2018; Sonnenschein et al., 2017). Top management support then strongly predicts alliance and collaboration ($\beta = 0.894$, $p < .001$; $R^2(CSAC) = 0.799$), supporting H6 and consistent with the expectation that executive backing is often required to formalize information-sharing

participation, allocate budgets for joint initiatives, and sustain inter-organizational security governance arrangements (Sonnenschein et al., 2017; Fransen et al., 2015). Taken together, these results validate a governance-to-collaboration pathway in which leadership cognition (risk perception) translates into leadership action (support), which, in turn, enables external engagement (collaboration) that materially strengthens internal capabilities.

Finally, the environmental turbulence pathway is partially supported. Market turbulence positively predicts top management risk perception ($\beta = 0.565$, $p < .001$; $R^2(CSTMRP) = 0.319$), supporting H8. In addition, this implies that volatile product–market conditions call managerial attention to risk vectors that may break continuity and performance, such as cyber risk (Jaworski & Kohli, 1993; Romanosky, 2016; Durst et al., 2024). Technological turbulence predicts market turbulence ($\beta = 0.832$, $p < .001$; $R^2(MT) = 0.692$), thereby supporting H9 and supporting the claim that fast and sudden technological change threatens customer expectations and competing offerings, enhancing the market volatility as well (Jaworski & Kohli, 1993; Bodlaj & Čater, 2019; Pratono, 2016). Technological turbulence, however, has no significant direct effect on cybersecurity risk maturity ($\beta = 0.020$, $p = 0.699$); therefore, H10 is rejected. This non-finding is instructive: it indicates that technological turbulence does not directly erode the institutionalization of maturity practices in large enterprises, and that its influence runs indirectly through market turbulence and managerial risk salience (the TT → MT → CSTMRP pathway). One plausible interpretation is that large firms' established governance structures and resourcing buffers may stabilize maturity processes even amid significant technological change, thereby mitigating the hypothesized negative direct effect (Durst et al., 2024; Kilani, 2020).

Table 30: SEM model regression coefficients

Outcome	Predictor	R-squared	Std. estimate	Std. Error	z-value	p	Hypothesis	Conclusion
CSA	CSAC	0.88	0.938	0.020	46.428	< .001	H5a	✓ (+1%)
CSAC	CSTMS	0.799	0.894	0.021	43.388	< .001	H6	✓ (+1%)
CSRC	CSAC	0.773	0.879	0.027	33.176	< .001	H4b	✓ (+1%)
CSRM	TI	0.874	0.477	0.098	4.893	< .001	H2a	✓ (+1%)

	CSRC		0.376	0.106	3.549	< .001	H2b	✓ (+1%)
	CSA		-0.200	0.157	-1.276	0.202	H3a	∅
	CST		0.336	0.173	1.942	0.052	H3b	✓(marg.+10%)
	TT		0.020	0.051	0.387	0.699	H10	∅
CST	CSAC	0.920	0.959	0.018	54.317	< .001	H5b	✓ (+1%)
CSTMRP	MT	0.319	0.565	0.063	8.985	< .001	H8	✓ (+1%)
CSTMS	CSTMRP	0.870	0.933	0.016	57.585	< .001	H7	✓ (+1%)
MT	TT	0.692	0.832	0.058	14.316	< .001	H9	✓ (+1%)
R	CSRM	0.934	0.967	0.020	48.372	< .001	H1	✓ (+1%)
TI	CSAC	0.702	0.838	0.035	24.129	< .001	H4a	✓ (+1%)

Source: Author's work

In summary, the research results provide strong empirical support for the central theoretical architecture: maturity is a dominant driver of resilience (H1), maturity is built primarily through technological infrastructure and cybersecurity resources (H2a, H2b), collaboration is a critical upstream engine that strengthens both technical and human-capability dimensions (H4a, H4b, H5a, H5b), and governance operates as a cascading mechanism from managerial risk perception to support to collaboration (H7, H6). The main deviations from the hypothesized structure concern the limited incremental role of awareness (H3a) and the absence of a direct turbulence-to-maturity effect (H10), both of which are consistent with the earlier evidence of strong construct proximity among human and governance dimensions and with a model in which turbulence operates chiefly through managerial perception channels rather than through direct capability degradation.

5.3. Discussion of research results

This chapter interprets the empirical findings in relation to the study's theoretical framework and prior research on cybersecurity risk management and organizational resilience. It synthesizes the implications of the SEM results for theory and practice. It highlights key

boundary conditions, limitations, and directions for future research based on the observed pattern of supported and unsupported hypotheses.

5.3.1. Theoretical contribution

This dissertation contributes to the cyber resilience and cyber risk management literature by empirically specifying and testing an integrated capability-governance framework that links cybersecurity risk maturity to organizational resilience in large enterprises. Building on foundational conceptualizations of cyber resilience as the capacity to anticipate, withstand, recover, and adapt to cyber disruption (Linkov & Kott, 2018), the study operationalizes cybersecurity risk maturity as an institutionalized lifecycle of risk identification, assessment, mitigation, and continuous improvement (Rajan et al., 2021). It demonstrates that maturity functions as a dominant proximal mechanism through which resilience is realized in the surveyed organizations. This strengthens theoretical arguments that resilience in the cyber domain is not only an outcome condition but is strongly grounded in routinised, governance-supported risk practices that translate strategic intent into consistent operational control.

A second contribution lies in integrating and empirically validating a multi-layered antecedent structure of maturity that combines technological, organizational, human, relational, and governance determinants. Prior work frequently discusses these domains in parallel (for example, infrastructure and control feasibility, resourcing and formalization, and human factors in secure behavior), but often without modeling their joint effects within a single structural system. By estimating these mechanisms simultaneously, the study clarifies that technological infrastructure and cybersecurity resources and capabilities constitute the primary "foundational" drivers of maturity, consistent with the argument that mature risk management depends on robust technical platforms, monitoring feasibility, and organizational capacity to implement and sustain controls (Van Laak, 2004; Subashini & Kavitha, 2011; Almuhammadi & Alsaleh, 2017; Landoll, 2021; Rajan et al., 2021). This positioning advances the literature beyond single-factor explanations by demonstrating how internal foundations operate within a broader governance-enabled capability architecture.

Third, the dissertation extends research on inter-organizational information sharing and collaborative security by treating alliances and collaborations as central mechanisms for capability building rather than as peripheral practices. Prior studies emphasize the importance of information-sharing communities and collaborative arrangements for threat management and the diffusion of security knowledge and practices (Fransen et al., 2015). Similarly, work on

multisource and security governance highlights the level of coordination required across organizational boundaries to maintain security in complex service ecosystems (Naicker & Mafaiti, 2019). The present model advances these streams by demonstrating that collaboration is theoretically and empirically positioned upstream of multiple internal capability domains, supporting an integrative view in which external collaboration is not merely informational, but materially shapes infrastructure capability, resource availability, and organizational learning processes that feed into maturity.

Fourth, the research contributes to the governance strand of cybersecurity studies by testing a cascading leadership mechanism in which top management's risk perception translates into support from top management, thereby enabling collaboration and subsequent capability development. This aligns with existing arguments that executive risk salience is a trigger for resource allocation, policy sponsorship, and governance embedding (Cebula et al., 2014; Rothrock et al., 2018; Sonnenschein et al., 2017), while also extending the literature by empirically locating collaboration as the principal organizational "deployment channel" through which governance attention becomes capability change. In theoretical terms, the model links managerial cognition (risk perception) to managerial action (support) and, in turn, to inter-organizational strategy (collaboration), thereby connecting governance theory with the operational reality of cyber capability development.

Fifth, by incorporating market and technological turbulence as contextual conditions shaping the governance pathway, the dissertation adds a new dimension to explanations of environmental contingency. Based on existing turbulence concepts in marketing and strategic management (Jaworski & Kohli, 1993; Bodlaj & Čater, 2019; Pratono, 2016), the model recontextualizes turbulence for cyber governance by suggesting that market turbulence leads to higher perceptions of risk by top management, and technological turbulence is a multiplier of market turbulence. It creates a theoretically relevant liaison between environmental dynamism and cyber governance mechanisms. Crucially, there appears to be no direct technological-turbulence effect on maturity, despite theoretical literature that asserts that rapid technological change enlarges attack surfaces and inhibits the consolidation of control (Kilani, 2020; Durst et al., 2024), provides rationale for the refinement that turbulence may influence maturity only indirectly among large firms through leadership attentiveness and emphasis, rather than by undermining the institutionalization of risk processes.

Finally, the research contributes to construct-level theory development by revealing empirical overlaps among conceptually related domains, particularly awareness and training, and the governance link between risk perception and support. In human factors studies, awareness and training are routinely considered closely related to secure behavior and organizational learning (Trim & Upton, 2013; Li et al., 2019; Moustafa et al., 2021; Cains et al., 2022). The present results reinforce the notion of coupling and suggest that, in practice, respondents may experience these as an integrated human-capability system rather than as sharply separable constructs. This motivates theoretically grounded future refinement, such as higher-order conceptualizations of human capability, more differentiated item design, or boundary-condition theorizing about when awareness operates independently of training.

5.3.2. Practical contributions

The empirical results present several practical implications for large companies seeking to build organizational resilience by implementing more mature cybersecurity risk management. In this sense, it indicates that resilience initiatives are most effective when translated into institutionalized risk-management routines rather than treated as isolated technical controls. Organizations seeking resilience gains should therefore prioritize formalizing lifecycle-oriented process: consistent risk identification, structured assessment, control implementation, monitoring, incident response, recovery, and continuous improvement, supported by clear ownership and governance.

A central practical implication concerns investment priorities in capabilities. The results show that technological infrastructure and cybersecurity resources and capabilities are the most consequential direct enablers of cybersecurity risk maturity. This supports an investment logic in which organizations ensure that core infrastructure is reliable, well-integrated, and secure, and that adequate human and organizational resources are available to operate and improve controls over time. Practically, this entails sustained investment in monitoring and detection capacity, secure architecture and system hardening, and the availability of specialized security roles and procedures that enable repeatable risk management rather than reactive, ad hoc actions.

The study also highlights that inter-organizational alliances and collaborations are not peripheral; they function as a powerful upstream mechanism that strengthens multiple internal capability domains simultaneously. For decision-makers, this implies that participation in structured information-sharing communities and collaborative security arrangements should be

treated as a strategic capability lever, not merely a compliance activity. Practical actions include formal membership in sectoral information-sharing and analysis centers, systematic threat intelligence exchange with trusted partners, joint incident exercises, shared response playbooks, and structured collaboration with suppliers and third parties on vulnerabilities and patches. In operational terms, these mechanisms can accelerate learning, improve situational awareness, and reduce the time required to translate emerging threat signals into internal control adjustments.

Governance-related implications are similarly clear. The results support a cascading pathway in which top management's risk perception drives top management support, which, in turn, enables collaboration and subsequent capability development. Practically, this indicates that cybersecurity programs benefit from explicit executive-level framing of cyber risk as a strategic and operational continuity risk, supported by governance routines that sustain attention over time. Organizations can operationalize this by integrating cyber risk into enterprise risk management reporting, board-level dashboards, and performance governance, and by clarifying executive accountability for cyber risk outcomes. In addition, explicit top-management sponsorship appears to be a precondition for sustaining external collaboration, suggesting that collaboration initiatives should be embedded within governance structures rather than delegated solely to technical units.

The results for human capability indicate a more nuanced implication. Awareness and training are closely linked to the broader capability system, but their incremental predictive effect on maturity diminishes when other enablers are considered. In practical terms, this does not mean that human capability is unimportant; rather, awareness and training are most effective when deeply embedded in organizational operational risk practices and through collaborative learning content. They might therefore focus on role-related and scenario-driven training that is directly tied to incident patterns, threat intelligence, and control needs, and that links training outputs to observable process behaviors such as reporting rates, policy compliance, and response readiness, rather than treating them as separate communications campaigns.

Regarding environmental turbulence, both results indicate that market turbulence tends to heighten the risk for top management and that technological turbulence tends to heighten market turbulence. In practice, organizations already operating in turbulent environments should expect cyber risk salience to increase further and can thus capitalize on this increased focus by building a stronger foundation for strengthening governance and risk management.

The absence of any effect of technological turbulence on maturity is also reflected in the observation that if governance and foundational capabilities are sufficiently institutionalized, enterprises with mature institutions can maintain a stable risk management process even during periods of rapid technological change. This provides a pragmatic strategic message: turbulence need not erode maturity if organizations invest in stabilizing risk processes and lifecycle management of controls. Considering these results and the strong interrelationships among the other constructs, the refined model presented in Figure 4 is empirically grounded.

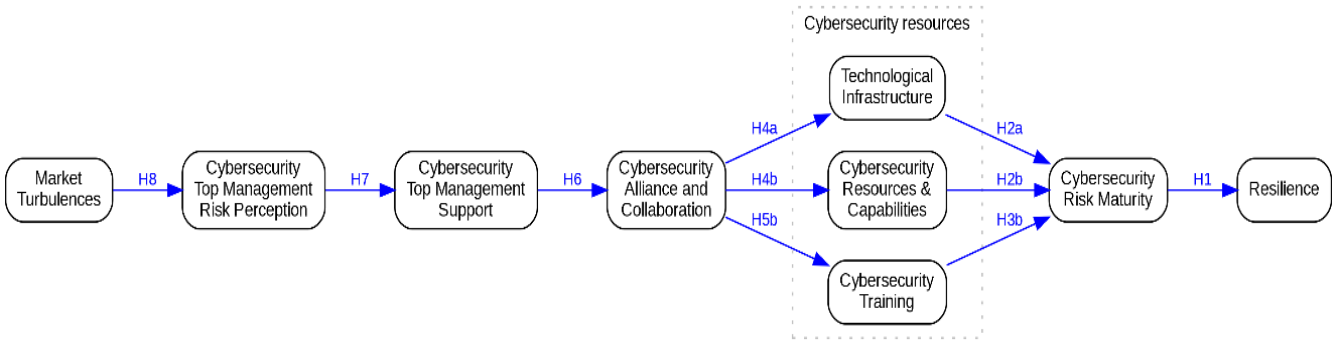


Figure 4: Final evidence-based model of cybersecurity-enabled organizational resilience

Source: Author's work

Taken together, the study provides a coherent set of managerial priorities. First, treat cybersecurity risk maturity as the primary operational pathway to resilience and organize programs around lifecycle routines. Second, prioritize investment in technological infrastructure and cybersecurity resources as foundational enablers of maturity. Third, institutionalize external collaboration as a strategic capability accelerator to strengthen internal resources, infrastructure, and organizational learning. Fourth, strengthen top-management risk framing and sponsorship mechanisms to enable sustained collaboration and investment in capabilities. These implications are directly actionable for boards, executive leadership, and cybersecurity governance functions seeking to translate resilience objectives into measurable, scalable organizational practices.

5.3.3. Research limitations and recommendations for future research

This study provides empirical evidence on the relationships among cybersecurity risk maturity, its organizational antecedents, and organizational resilience in large Swiss enterprises. The findings should nevertheless be interpreted considering several methodological and design limitations that also point to concrete directions for future research.

First, the study relies on cross-sectional survey design. Although the hypothesized relationships are grounded in theory and the estimated structural model is internally coherent, cross-sectional data limit the strength of causal inference and preclude assessment of temporal sequencing. Future research should employ longitudinal designs (for example, repeated measurement waves) to test whether changes in governance, collaboration, and internal capabilities precede and predict subsequent changes in cybersecurity risk maturity and resilience, and to examine dynamic feedback processes (for example, whether incidents trigger increases in top management risk perception and subsequent capability investment).

Second, common method variance remains a potential concern because predictors and outcomes were measured using the same instrument and collected from the same respondents at the same time. While the study targeted respondents with appropriate organizational oversight and included multiple constructs with differentiated measurement properties, common-source bias can still inflate relationships, particularly among conceptually adjacent governance and human-capability constructs. Future studies should consider multi-informant designs (for example, separating governance responses from operational/technical responses), temporally separating measures, and including marker variables or alternative measurement strategies to mitigate common method effects.

Third, the findings are based on a single-country setting and a specific organizational segment (large enterprises operating in Switzerland). Switzerland has distinctive regulatory, sectoral, and institutional features that may shape cyber governance and collaboration norms. External validity may therefore be limited, particularly for small and medium-sized enterprises or for organizations operating in institutional contexts with different regulatory intensity, market structures, and cyber threat profiles. Future research should replicate the model in other national settings and compare results across countries and extend the framework to small and medium-sized enterprises to test whether resource constraints and governance structures alter the relative importance of collaboration, training, and infrastructural foundations.

Fourth, the achieved sample size (n = 170) is adequate for the estimated model but remains modest relative to the number of constructs and parameters in a multi-path structural equation model. This can reduce statistical power for smaller effects and may partly explain borderline results, such as the weaker evidence for the training-to-maturity relationship. Future research should seek larger sample sizes to enable more stable estimates, narrower confidence intervals, and formal multi-group comparisons.

Fifth, several constructs are conceptually proximate and empirically highly correlated, particularly cybersecurity awareness and training, and top management risk perception and support. Although the measurement model demonstrated acceptable overall psychometric quality, the high proximity suggests partial overlap in how respondents differentiate between these domains in practice. Future research should refine and expand item pools to better capture the conceptual boundaries between adjacent constructs, consider modeling higher-order factors (for example, a second order "human capability" factor combining awareness and training), and assess measurement invariance across sectors and respondent roles.

Sixth, the operationalization of environmental turbulence necessitated item reduction, yielding relatively narrower representations of market and technological turbulence. This may limit the breadth of inference about "turbulence" and could contribute to the non-significant direct effect of technological turbulence on maturity. Future studies should consider alternative operationalizations of turbulence, including objective proxies (for example, sector-level technology turnover, volatility indices, or innovation adoption rates), richer multi-item scales, and industry-specific turbulence measures. In addition, future research should explicitly test moderation effects (rather than only direct effects) to examine whether turbulence strengthens or weakens the relationships among governance, capabilities, maturity, and resilience.

Seventh, the model does not explicitly incorporate potentially relevant organizational controls and boundary conditions, such as regulatory exposure, prior incident experience, outsourcing intensity, group-level governance centralization, or third-party risk complexity. Although the questionnaire collected several contextual variables (e.g., incident experience, monitoring arrangements, assessments, and business continuity testing), these were not fully integrated into the SEM as moderators or controls. Future research should incorporate these conditions to test whether the pathways differ between organizations with recent significant incidents and those without, between internal and outsourced monitoring arrangements, and between group-affiliated and standalone enterprises.

Eighth, the reliance on self-reported perceptual data may be exposed to social desirability bias. The descriptive statistics indicate that self-assessments remain favorable, as most construct means and averages are well above the midpoint. Some respondents, especially leaders, may exaggerate their establishment's competence in a delicate field such as cybersecurity. This possible positive self-assessment bias may inflate the mentioned levels of maturity and resilience. To obtain a more objective view, further studies should correlate perceptual data with objectively defined proxies of cybersecurity performance, such as independent audit ratings, information from security ratings services, or metrics such as MTTD and mean time to respond.

Overall, these limitations do not undermine the study's core contribution, but they delineate the scope of inference. Future research that combines longitudinal and multi-informant designs, incorporates objective indicators of maturity and resilience, broadens the cross-country and cross-size scope, and refines the measurement of proximate and contextual constructs would provide a more comprehensive and causally informed understanding of how cybersecurity risk maturity develops and how it translates into organizational resilience.

6. CONCLUSION

This doctoral study examined several factors that promote organizational resilience, with a specific focus on the predictive role of cybersecurity risk maturity. The preceding chapters have systematically elaborated a theoretical model, formulated its constructs, and tested them within an empirical framework that was extensively validated using structural equation modeling (SEM) with 170 senior respondents with cybersecurity oversight at large Swiss enterprises. This concluding chapter summarizes the research trajectory, from empirical findings to conceptual and practical findings.

Empirical evidence, as discussed in Chapter 5, provided a nuanced interpretation of the developed theoretical model. A refinement of the initial model is required because certain pathways were not statistically significant, despite extensive verification of the general framework. Based on these findings, the final evidence-based model of resilience is illustrated in Figure 4, which presents a logical, empirically supported pathway for developing resilience within large organizations amid a turbulent digital environment. Testing the initial conceptual model, two hypotheses derived from the SEM results were not supported: Cybersecurity Awareness did not have a significant direct effect on Cybersecurity Risk Maturity (H3a: $\beta = -0.200$, $p = 0.202$), and Technological Turbulence did not have a significant direct effect on Cybersecurity Risk Maturity (H10: $\beta = 0.020$, $p = 0.699$). Technological turbulence has no significant direct effect on cybersecurity risk maturity (H10) but is retained in the model as an upstream environmental factor because it significantly increases market turbulence (H9), which in turn activates the governance and leadership pathway. Technological turbulence is therefore one of several sources of market turbulence rather than its only cause.

A carefully refined model clearly articulates a defined sequential chain of impacts from external environmental effects, culminating in increased organizational resilience. The derived hypotheses can be logically organized into three fundamental pathways:

1. The Governance and Leadership Pathway (H8, H7, H6): The model validates that external Market Turbulence is the major factor leading to an increase in the Cybersecurity Top Management Risk Perception (H8: $\beta = 0.565$, $p < .001$). This perceived risk was the strongest predictor of securing Cybersecurity Top Management Support (H7: $\beta = 0.933$, $p < .001$). This executive support is instrumental in creating Cybersecurity Alliance and Collaboration (H6: $\beta = 0.894$, $p < .001$). This pathway

underscores a critical management sequence: market volatility alerts leadership, mobilizes support, and then produces joint defense strategies. This path indicates that resilience is not a purely technical issue; it also begins with strategic, top-down governance mechanisms implemented in response to external pressures.

2. Collaborative Capability Pathway (H4a, H4b, H5b): The findings determine Cybersecurity Alliance and Collaboration as an exemplar, strategic catalyst. This collaboration posture is a strong predictor for developing Technological Infrastructure (H4a: $\beta = 0.838$, $p < .001$), building internal Cybersecurity Resources & Capabilities (H4b: $\beta = 0.879$, $p < .001$), strengthening Cybersecurity Awareness (H5a: $\beta = 0.938$, $p < .001$), and upgrading Cybersecurity Training (H5b: $\beta = 0.959$, $p < .001$). This demonstrates that enterprises do not construct their defenses in isolation. Rather, it is the interaction with external ecosystems (e.g., ISACs, threat intelligence platforms) itself that most significantly fosters the development of a firm's internal technical, human, and resource-based capabilities.
3. The Maturity and Resilience Pathway (H2a, H2b, H3b, H1): The model shows that Cybersecurity Risk Maturity is a multi-dimensional capability built upon core structural components. Both Technological Infrastructure (H2a: $\beta = 0.477$, $p < .001$) and Cybersecurity Resources & Capabilities (H2b: $\beta = 0.376$, $p < .001$) are robust, significant predictors of maturity. Cybersecurity Training (H3b: $\beta = 0.336$, $p = 0.052$) also showed a positive association that was marginally significant at the 10% level. The study validates its main hypothesis that Cybersecurity Risk Maturity has substantial predictive value for Organizational Resilience (H1: $\beta = 0.967$, $p < .001$), accounting for 93.4% of the variance in resilience ($R^2 = 0.934$). This strongly suggests that a mature, risk-based cybersecurity posture should be viewed not solely as a defensive function but as a critical enabler of an enterprise's ability to sustain operations and recover from disruption.

While the rejection of two hypotheses is theoretically informative, the confirmation of the remaining hypotheses provides equally significant insights. The absence of a significant direct effect of Cybersecurity Awareness on Cybersecurity Risk Maturity (H3a) is particularly noteworthy. It implies that general awareness campaigns may not be sufficient on their own to drive maturity. Although awareness is strongly influenced by collaboration (support for H5a), its effect on maturity may be indirect, mediated by other factors, such as integration into formal training and capability development. This research empirically confirms an important

distinction, supporting frameworks that distinguish between general awareness and formal, skill-based instruction (e.g., Paulsen et al., 2012; NIST, 2024). The results indicate that Cybersecurity Awareness, a general state of employee vigilance, is not directly an indicator of risk maturity. Rather, maturity is more closely associated with Cybersecurity Training, a formal, structured process that focuses on developing verifiable skills and competencies (Chowdhury et al., 2022; Durst et al., 2024). The data suggest that organizations reach maturity not solely through broad awareness campaigns, but through targeted, measurable training interventions designed, assessed, and continuously improved as part of a formal program (He & Zhang, 2019).

Likewise, the non-significant direct effect of Technological Turbulence on Cybersecurity Risk Maturity (H10) indicates that technological change alone may not directly drive the maturation of an organization's risk posture. In fact, Market Turbulence and related subsequent shifts in leadership perception and support serve as mediating gateways for these effects. This implies that it is not technological change itself, but the competition and market-driven pressures it engenders that organizations respond to.

This dissertation makes several contributions to academic literature on cybersecurity, strategic management, and organizational resilience. It proposes and empirically tests a coherent multilevel model that links external environmental factors to internal governance and capabilities, and ultimately to overall organizational outcomes. It offers a more comprehensive theoretical perspective than existing theories that have focused primarily on narrower technical or procedural aspects of cybersecurity, incorporating concepts from the Dynamic Capabilities View and theoretical institutional frameworks, such as institutional theory.

Second, the study specifies the ordering of relationships underlying resilience development. The refined model (Figure 4) presents a clear, empirically supported sequence consistent with the data: market turbulence is associated with heightened executive risk perception and support, which in turn is associated with collaborative engagement and with internal capabilities underpinning risk maturity. Because the design is cross-sectional, this sequence is theoretically motivated rather than causally established. This offers a systematic, evidence-based approach that moves theory beyond simple taxonomies of critical success factors.

Third, the results on the non-significant contribution of general awareness (H3a) and the indirect role of technological turbulence (H10) provide an important theoretical enhancement. It challenges prevailing assumptions in literature and underscores the need for mediated effects

and contextual triggers (e.g., market pressure). Perhaps the most important contribution to theoretical understanding is the primary, mediating function of Cybersecurity Alliance and Collaboration, which, as a principal construct, converts executive intent into capability development.

Finally, this study makes a strong theoretical contribution by demonstrating the strong predictive power of Cybersecurity Risk Maturity for Organizational Resilience ($R^2 = 0.934$). Its focus elevates cybersecurity beyond a cost- or compliance-centric function to a strategic cornerstone of the modern enterprise's viability. The findings of this research offer clear, actionable guidance for the executives and cybersecurity practitioners of large organizations, and can be summarized as follows:

1. **Focus on market signals to garner executive support:** Cybersecurity leaders need to build support from executives and gain their buy-in by framing initiatives not in technical terms but in terms of market turbulence and competitive risk. As the data demonstrates, leadership is responsive to market pressures (H8); hence, this is the most potent lever for mobilizing support (H7).
2. **Prioritize and invest in collaborative defense:** The model unequivocally identifies external collaboration (CSAC) as the single most important driver for building internal capabilities (H4a, H4b, H5b). Managers should therefore prioritize investments in active participation in ISACs, threat intelligence sharing platforms, and peer-to-peer alliances. Collaboration is not an adjunct to a security program; it is its primary engine.
3. **Move beyond awareness to embedded training:** The results indicate that the budget allocated to generic awareness campaigns may yield limited returns in terms of risk maturity. Organizations could instead build awareness principles into their structured capability-focused Cybersecurity Training programs (H3b), as these programs exhibit a more direct, albeit marginal, correlation with maturity.
4. **Treat cybersecurity risk maturity as a core business objective:** The strong predictive power of CSRM on organizational resilience (H1) provides a clear rationale for boards and C-suites to prioritize it. Cybersecurity maturity is not an IT metric; it is a core indicator of the business's ability to survive and prosper. It should be managed, measured, and reported with the same rigor as financial performance.

This research aimed to move beyond theoretical generalizations and develop an empirically validated blueprint for achieving this resilience. The results reveal a powerful and explicit

pathway: resilience is not built solely by the technology itself, but by a structured alignment of leadership, collaboration, and capability. It starts with market-responsive executives advocating for a collaborative defense posture, thereby creating mature, risk-based cyber capabilities that underpin an effective, resilient enterprise. This refined model advances current theory and offers a practical strategic guide for organizations navigating the turbulent digital landscape of the 21st century.

List of tables

List of figures

List of abbreviations

Business Continuity Planning (BCP)

Chief Information Security Officer (CISO)

Comparative Fit Index (CFI)

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Cybersecurity Alliance and Collaboration (CSAC)

Cybersecurity and Infrastructure Security Agency (CISA)

Cybersecurity Awareness (CSA)

Cybersecurity Framework (CSF)

Cybersecurity Resources and Capabilities (CSRC)

Cybersecurity Risk Maturity (CSRM)

Cybersecurity Top Management Risk Perception (CSTMRP)

Cybersecurity Top Management Support (CSTMS)

Cybersecurity Training (CST)

Digital Operational Resilience Act (DORA)

European Union Agency for Network and Information Security (ENISA)

Factor Analysis of Information Risk (FAIR)

Federal Emergency Management Agency (FEMA)

Federal Financial Institutions Examination Council (FFIEC)

Federal Office for Cybersecurity (BACS)

General Data Protection Regulation (GDPR)

Health Insurance Portability and Accountability Act (HIPAA)

Heterotrait-Monotrait Ratio (HTMT)

Information Sharing and Analysis Centers (ISACs)

International Information System Security Certification Consortium ((ISC)²)

International Organization for Standardization (ISO)

Key Performance Indicators (KPIs)

Key Risk Indicators (KRIs)

Market Turbulences (MT)

Mean Time to Detect (MTTD)

Mean Time to Respond (MTTR)

National Cyber Security Centre (NCSC)

National Initiative for Cybersecurity Education (NICE)

National Institute of Standards and Technology (NIST)

Network and Information Security Directive (NIS2)

Recovery Point Objective (RPO)

Recovery Time Objective (RTO)

Root Mean Square Error of Approximation (RMSEA)

Standardized Root Mean Square Residual (SRMR)

Structural Statistics of Enterprises (STATENT)

Structural Equation Modeling (SEM)

Swiss Financial Market Supervisory Authority (FINMA)

Technological Infrastructure (TI)

Technological Turbulences (TT)

The Open Group Architecture Framework (TOGAF)

Tucker-Lewis Index (TLI)

References

1. Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939–953. https://doi.org/10.1002/asi.24311

2. Ahmad, M. R., Osman, M. H., Abdullah, A., & Sharif, K. Y. (2024). Evolution of Information Security Awareness Towards Maturity: A Systematic Review. International *Journal on Advanced Science, Engineering and Information Technology, 14*(5), 1738–1747. https://doi.org/10.18517/ijaseit.14.5.20234

3. Alagic, G., Dang, Q., Moody, D., Robinson, A., Silberg, H., & Smith-Tone, D. (2024). Module-lattice-based key-encapsulation mechanism standard (FIPS 203). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.FIPS.203

4. Al-Sartawi, A. M. A. M. (2020). Information technology governance and cybersecurity at the board level. *International Journal of Critical Infrastructures*, *16*(2), 150–161. https://doi.org/10.1504/IJCIS.2020.107265

5. Aldea, C. L., Bocu, R., & Solca, R. N. (2023). Real-Time Monitoring and Management of Hardware and Software Resources in Heterogeneous Computer Networks Through an Integrated System Architecture. *Symmetry*, *15*(6), 1134. https://doi.org/10.3390/sym15061134

6. Alexander, D. (2005). Towards the development of a standard in emergency planning. *Disaster Prevention and Management*, *14*(2), 158–175. https://doi.org/10.1108/09653560510595164

7. Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. *Applied Sciences*, *10*(10), 3660. https://doi.org/10.3390/app10103660

8. Allen, P. C. (2023). Surviving the storm: The key to cyber resilience and incident response in healthcare. *Healthcare Management Forum*, *37*(1), 26–29. https://doi.org/10.1177/08404704231187103

9. Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for the NIST cybersecurity framework. In D. C. Wyld, J. Zizka, & D. Nagamalai (Eds.), *Computer Science & Information Technology (CS & IT)* (pp. 51–62). https://doi.org/10.5121/csit.2017.70305

10. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98,* 102003. https://doi.org/10.1016/j.cose.2020.102003

11. Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, *103*(3), 411–423. https://doi.org/10.1037/0033-2909.103.3.411

12. Arbanas, K., Spremić, M., & Zajdela Hrustek, N. (2021). Holistic framework for evaluating and improving information security culture. *Aslib Journal of Information Management, 73*(5), 699–719. https://doi.org/10.1108/AJIM-02-2021-0037

13. Assenza, G., Ortalda, A., & Setola, R. (2024). Redefining systemic cybersecurity risk in interconnected environments. *Applied Cybersecurity & Internet Governance*, *4*(2). https://doi.org/10.60097/ACIG/192119

14. Assibi, A. T. (2023). Literature review on building cyber resilience capabilities to counter future cyber threats: The role of enterprise risk management (ERM) and business continuity (BC). *Open Access Library Journal*, *10*(4), 1–15. https://doi.org/10.4236/oalib.1109882

15. Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: Context and shared concepts. *Journal of Cyber Policy*, *3*(2), 258–283. https://doi.org/10.1080/23738871.2018.1520271

16. Bajgorić, N., Spremić, M., & Turulja, L. (2013). Implementation of IT governance standards and business continuity management in transition economies: The case of banking sector in Croatia and Bosnia-Herzegovina. *Ekonomska istraživanja – Economic Research, 26*(1), 183–202.

17. Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities

and challenges toward responsible AI. *Information Fusion*, *58,* 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

18. Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological Bulletin, 107*(2), 238–246. https://doi.org/10.1037/0033-2909.107.2.238
19. Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: The concept, a literature review and future directions. *International Journal of Production Research*, *49*(18), 5375–5393. https://doi.org/10.1080/00207543.2011.563826
20. Black, W., & Babin, B. J. (2019). *Multivariate data analysis: Its approach, evolution, and impact.* In B. J. Babin & M. Sarstedt (Eds.), The great facilitator: Reflections on the contributions of Joseph F. Hair, Jr. to marketing and business research (pp. 121–130). Springer. https://doi.org/10.1007/978-3-030-06031-2_16
21. Bodlaj, M., & Čater, B. (2019). The impact of environmental turbulence on the perceived importance of innovation and innovativeness in SMEs. *Journal of Small Business Management*, *57*(S2), 417–435. https://doi.org/10.1111/jsbm.12482
22. Bollen, K. A. (1989). *Structural Equations with Latent Variables.* Wiley. https://doi.org/10.1002/9781118619179
23. Brezavšček, A., & Baggia, A. (2025). Recent trends in information and cyber security maturity assessment: A systematic literature review. *Systems*, *13*(1), 52. https://doi.org/10.3390/systems13010052
24. Brown, T. A. (2015). *Confirmatory factor analysis for applied research* (2nd ed.). Guilford Press.
25. Browne, M. W., & Cudeck, R. (1993). Alternative ways of assessing model fit. In K. A. Bollen & J. S. Long (Eds.), *Testing structural equation models* (pp. 136–162). Sage Publications.
26. Burch, G. F., Burch, J., & McGarry, M. (2024). Cybersecurity risk management governance: An agency theory perspective. *ISACA*, Issue 5. https://www.isaca.org/resources/isaca-journal/issues/2024/volume-5/cybersecurity-risk-management-governance
27. Burnard, K., & Bhamra, R. (2011). Organisational resilience: Development of a conceptual framework for organisational responses. *International Journal of*

Production Research, *49*(18), 5581–5599. https://doi.org/10.1080/00207543.2011.563827

28. Business Continuity Institute. (2024). *Good Practice Guidelines (GPG)* 7.0 edition. https://www.thebci.org/certification-training/good-practice-guidelines.html
29. Büyüközkan, G., & Güler, M. (2025). Cybersecurity maturity model: Systematic literature review and a proposed model. *Technological Forecasting and Social Change*, *213*, 123996. https://doi.org/10.1016/j.techfore.2025.123996
30. Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, *42*(8), 1643–1669. https://doi.org/10.1111/risa.13687
31. Carías, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic approach to cyber resilience operationalization in SMEs. *IEEE Access*, *8,* 174200–174221. https://doi.org/10.1109/ACCESS.2020.3026063
32. Cebula, J. J., Popeck, M. E., & Young, L. R. (2014). A taxonomy of operational cyber security risks version 2 (CMU/SEI-2014-TN-006). *Software Engineering Institute*. https://doi.org/10.21236/ada609863
33. CEN. (2018). CEN/TS 17091:2018 Crisis management - Guidance for developing a strategic capability. European Committee for Standardization.
34. Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity*, *8*(1), tyac006. https://doi.org/10.1093/cybsec/tyac006
35. Cheimonidis, P., & Rantos, K. (2023). Dynamic risk assessment in cybersecurity: A systematic literature review. *Future Internet*, *15*(10), 324. https://doi.org/10.3390/fi15100324
36. Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS Quarterly*, *36*(4), 1165–1188. https://doi.org/10.2307/41703503
37. Cherdantseva, Y., & Hilton, J. (2013). A reference model of information assurance & security. 2013 *International Conference on Availability, Reliability and Security (ARES)* (pp. 546–555). IEEE. https://doi.org/10.1109/ARES.2013.72

38. Chowdhury, N., Katsikas, S., & Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security*, *113,* 102551. https://doi.org/10.1016/j.cose.2021.102551

39. Christensen, C. M. (1997). The innovator's dilemma: When new technologies cause great firms to fail. *Harvard Business School Press*. https://www.hbs.edu/faculty/Pages/item.aspx?num46

40. Christopher, M., & Peck, H. (2004). Building the resilient supply chain. The *International Journal of Logistics Management*, *15*(2), 1–13. https://doi.org/10.1108/09574090410700275

41. Cohen, J. (1988). Statistical power analysis for the behavioral sciences (2nd ed.). *Routledge*. https://doi.org/10.4324/9780203771587

42. Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise risk management: Integrating with strategy and performance. https://www.coso.org/guidance-erm

43. Conklin, W. A., Shoemaker, D., & Kohnke, A. (2017). Cyber resilience: Rethinking cybersecurity strategy to build a cyber resilient architecture. In A. R. Bryant, R. F. Mills, & J. Lopez. (Eds.), *Proceedings of the 12th International Conference on Cyber Warfare and Security (ICCWS 2017)* (pp. 105–111). Academic Conferences and Publishing International Ltd.

44. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

45. Craighead, C. W., Blackhurst, J., Rungtusanatham, M. J., & Handfield, R. B. (2007). The severity of supply chain disruptions: Design characteristics and mitigation capabilities. *Decision Sciences*, *38*(1), 131–156. https://doi.org/10.1111/j.1540-5915.2007.00151.x

46. Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, *16*(3), 297–334. https://doi.org/10.1007/BF02310555

47. Cybersecurity and Infrastructure Security Agency. (2020). *CRR: Method description and self-assessment user guide (Version 4.0).* U.S. Department of Homeland Security.

https://www.cisa.gov/sites/default/files/publications/2_CRR%204.0_Self-Assessment_User_Guide_April_2020.pdf

48. Cybersecurity and Infrastructure Security Agency. (2023a). *CISA cybersecurity strategic plan: FY2024–2026.* U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/2023-08/CISA_Cybersecurity_Strategic_Plan_FY2024-2026_508c.pdf

49. Cybersecurity and Infrastructure Security Agency. (2023b). *Zero trust maturity model: Version 2.0.* U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf

50. Cybersecurity and Infrastructure Security Agency. (2024). *Cross-sector cybersecurity performance goals* (Version 2.0). https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0

51. Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security* Review, *31*(2), 243–256. https://doi.org/10.1016/j.clsr.2015.01.005

52. Dal Cin, P., Kendzior, D., & Seedat, Y. (2025). State of cybersecurity resilience 2025. Accenture. State of Cybersecurity Resilience 2025 | Accenture

53. Dash, B., & Ansari, M. F. (2022). An effective cybersecurity awareness training model: First defense of an organizational security strategy. *International Research Journal of Engineering and Technology*, *9*(4), 1–6. https://www.irjet.net/archives/V9/i4/IRJET-V9I401.pdf

54. Davison, C. B. (2008). *Leadership characteristics as determinants of business continuity and disaster recovery planning: A correlational research investigation within institutions of higher education* (Doctoral dissertation, Capella University).

55. Deloitte. (2023). 2023 global future of cyber survey. *Deloitte*. Global Future of Cyber Survey 2023 | Deloitte Schweiz

56. Deming, W. E. (2000). *The New Economics for Industry, Government, Education* (2nd ed.). *MIT Press*. https://mitpress.mit.edu/9780262541169/the-new-economics-for-industry-government-education/

57. Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity*, *5*(1), tyz013. https://doi.org/10.1093/cybsec/tyz013

58. Durst, S., Hinteregger, C., & Zieba, M. (2024). The effect of environmental turbulence on cyber security risk management and organizational resilience. *Computers & Security*, *137,* 103591. https://doi.org/10.1016/j.cose.2023.103591

59. Ebert, N., Schaltegger, T., Ambuehl, B., Geppert, T., Trammell, A., Knieps, M., & Zimmermann, V. (2025). Learning from safety science: Designing incident reporting systems in cybersecurity. *Journal of Cybersecurity*, *11*(1). https://doi.org/10.1093/cybsec/tyaf019

60. economiesuisse. (2023). Swiss code of best practice for corporate governance. https://www.economiesuisse.ch/en/publications/swiss-code-best-practice-corporate-governance

61. Elliott, D., Swartz, E., & Herbane, B. (2010). *Business Continuity Management: A Crisis Management Approach* (2nd ed.). Routledge. https://doi.org/10.4324/9780203866337

62. European Commission. (2023). Commission guidelines on the application of Article 4(1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive). https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive

63. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119/1--88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

64. European Parliament and Council of the European Union. (2022a). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union, L 333. https://eur-lex.europa.eu/eli/reg/2022/2554/oj

65. European Parliament and Council of the European Union. (2022b). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of

cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union, L 333. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

66. European Union. (2024). Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2024/2847/oj

67. European Union Agency for Network and Information Security. (2018). Information-sharing and analysis centers (ISACs): Cooperative models. https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

68. European Union Agency for Cybersecurity. (2025). Handbook for cyber stress tests. https://www.enisa.europa.eu/publications/handbook-for-cyber-stress-tests

69. Fahey, E. (2024). The evolution of EU–US cybersecurity law and policy: On drivers of convergence. Journal of European Integration, *46*(7), 1073–1088. https://doi.org/10.1080/07036337.2024.2411240

70. FAIR Institute. (2024). FAIR-CRQ: Cyber risk quantification methodology. https://www.fairinstitute.org/

71. Federal Assembly of the Swiss Confederation. (2023). Federal Act on Data Protection (FADP) of 25 September 2020 https://www.fedlex.admin.ch/eli/cc/2022/491/en

72. Federal Council. (2023). National Cyberstrategy (NCS) 2023–2027. National Cyber Security Centre NCSC. https://www.ncsc.admin.ch/dam/ncsc/en/dokumente/strategie/cyberstrategie-ncs/Nationale-Cyberstrategie-NCS-2023-04-13-EN.pdf.download.pdf/Nationale-Cyberstrategie-NCS-2023-04-13-EN.pdf

73. Federal Emergency Management Agency. (2018). Continuity guidance circular (2024 Update). https://www.fema.gov/sites/default/files/documents/fema_continuity-guidance-circular_082024.pdf

74. Federal Financial Institutions Examination Council. (2017). Cybersecurity assessment tool. https://ithandbook.ffiec.gov/it-booklets/information-security

75. Federal Financial Institutions Examination Council. (2019). Business continuity management. https://ithandbook.ffiec.gov/it-booklets/business-continuity-management.aspx

76. Federal Office for National Economic Supply. (2023). *Minimum standard for improving ICT resilience.* https://www.ncsc.admin.ch/dam/ncsc/en/dokumente/infos-unternehmen/ikt-minimalstandards/ikt-minimalstandard-2023-en.pdf.download.pdf/ikt-minimalstandard-2023-en.pdf

77. Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernández-Gago, C., López, J., Markatos, E., Islami, L., & Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications*, *61,* 102916. https://doi.org/10.1016/j.jisa.2021.102916

78. Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture, and awareness. *Computers & Security*, *59,* 26–44. https://doi.org/10.1016/j.cose.2016.01.004

79. Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50. https://doi.org/10.1177/002224378101800104

80. Fransen, F., Smulders, A., & Kerkdijk, R. (2015). Cyber security information exchange to gain insight into the effects of cyber threats and incidents. *Elektrotechnik und Informationstechnik*, *132*(2), 106–112. https://doi.org/10.1007/s00502-015-0289-2

81. Freeman, R. E., Phillips, R., & Sisodia, R. (2020). Tensions in stakeholder theory. *Business & Society*, *59*(2), 213–231. https://doi.org/10.1177/0007650318773750

82. Freund, J., & Jones, J. (2014). *Measuring and managing information risk: A FAIR approach.* Butterworth-Heinemann.

83. Gartner. (2023). Key behaviors driving CISO effectiveness. https://www.gartner.com/en/documents/6048999

84. Geismann, J., Gerking, C., & Bodden, E. (2018). Towards ensuring security by design in cyber-physical systems engineering processes. *International Conference on Software and System Process (ICSSP 2018)* (pp. 123–127). ACM. https://doi.org/10.1145/3202710.3203159

85. Gibb, F., & Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management*, 26(2), 128–141. https://doi.org/10.1016/j.ijinfomgt.2005.11.008

86. Glaspie, H. W., & Karwowski, W. (2018). Human factors in information security culture: A literature review. *Advances in Intelligent Systems and Computing* (pp. 269–280). Springer, Cham. https://doi.org/10.1007/978-3-319-60585-2_25

87. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC), 5*(4), 438–457. https://doi.org/10.1145/581271.581274

88. Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: Insights from the Gordon–Loeb model. *Journal of Information Security, 7*(2), 49–59. https://doi.org/10.4236/jis.2016.72004

89. Hammer, M., & Champy, J. (2006). *Reengineering the corporation: A manifesto for business revolution.* HarperBusiness.

90. Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., & Koshutanski, H. (2020). Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. *Applied Sciences*, *10*(16), 5702. https://doi.org/10.3390/app10165702

91. He, M., Devine, L., & Zhuang, J. (2017). Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach. *Risk Analysis*, *38*(2), 215–225. https://doi.org/10.1111/risa.12878

92. He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249–257. https://doi.org/10.1080/10919392.2019.1611528

93. Henseler, J., Ringle, C. M., & Sarstedt, M. (2014). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

94. Herbane, B. (2010a). The evolution of business continuity management: A historical review of practices and drivers. *Business History*, *52*(6), 978–1002. https://doi.org/10.1080/00076791.2010.511185

95. Herbane, B. (2010b). Small business research: Time for a crisis-based view. *International Small Business Journal*, *28*(1), 43–64. https://doi.org/10.1177/0266242609350804

96. Hiatt, C. J. (2011). *A primer for disaster recovery planning in an IT environment.* IGI Global.

97. Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. *Procedia Manufacturing, 44*, 655–662. https://doi.org/10.1016/j.promfg.2020.02.243

98. Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, *6*(1), 1–55. https://doi.org/10.1080/10705519909540118

99. Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, *13*(4), 247–255. https://doi.org/10.1016/j.istr.2008.10.010

100. Institute of Risk Management. (2021). Operational Resilience. IRM.

101. International Organization for Standardization. (2016). Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation (ISO/IEC 27004:2016). https://www.iso.org/standard/64120.html

102. International Organization for Standardization. (2018). Risk management — Guidelines (ISO 31000:2018). https://www.iso.org/standard/65694.html

103. International Organization for Standardization. (2022a). Information security, cybersecurity and privacy protection — Guidance on managing information security risks (ISO/IEC 27005:2022). https://www.iso.org/standard/80585.html

104. International Organization for Standardization. (2022b). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/82875.html

105. International Organization for Standardization. (2022c). Security and resilience — Crisis management — Guidelines (ISO 22361:2022). https://www.iso.org/standard/50267.html

106. International Organization for Standardization. (2023). Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response (ISO/IEC 27035-2:2023). https://www.iso.org/standard/78974.html

107. International Organization for Standardization. (2019). Security and resilience—Business continuity management systems—Requirements (ISO Standard No. 22301:2019). https://www.iso.org/standard/75106.html

108. ISACA. (2022). State of cybersecurity 2022: Global update on workforce efforts, resources and cyberoperations. https://www.isaca.org/resources/reports/state-of-cybersecurity-2022

109. (ISC)². (2023). Cybersecurity workforce study 2023: Looking for the next generation of talent. https://www.isc2.org/Research/Workforce-Study

110. Ivanov, D. (2020). Predicting the impacts of epidemic outbreaks on global supply chains: A simulation-based analysis on the coronavirus outbreak (COVID-19/SARS-CoV-2) case. *Transportation Research Part E: Logistics and Transportation Review*, *136,* 101922. https://doi.org/10.1016/j.tre.2020.101922

111. Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems*, *28*(1), 66–82. https://doi.org/10.1016/j.jsis.2018.09.003

112. Järveläinen, J., Dang, D., Mekkanen, M., & Vartiainen, T. (2025). Towards a framework for improving cyber security resilience of critical infrastructure against cyber threats: A dynamic capabilities approach. *Journal of Decision Systems*. Advance online publication. https://doi.org/10.1080/12460125.2025.2479546

113. Jaworski, B. J., & Kohli, A. K. (1993). Market orientation: Antecedents and consequences. *Journal of Marketing*, *57*(3), 53–70. https://doi.org/10.2307/1251854

114. Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity. 2019 IEEE *5th International*

Conference on Collaboration and Internet Computing (CIC 2019) (pp. 209–218). https://doi.org/10.1109/CIC48465.2019.00047

115. Jerman, A., Bertoncelj, A., Dominici, G., Pejić Bach, M., & Trnavčević, A. (2020). Conceptual Key Competency Model for Smart Factories in Production Processes. *Organizacija*, *53*(1), 68–79. https://doi.org/10.2478/orga-2020-0005

116. Jiang, Y., Ritchie, B. W., & Verreynne, M. L. (2019). Building tourism organizational resilience to crises and disasters: A dynamic capabilities view. *International Journal of Tourism Research*, *21*(6), 882–900. https://doi.org/10.1002/jtr.2312

117. Jones, J. A. (2006). An Introduction to Factor Analysis of Information Risk (FAIR). *Norwich University Journal of Information Assurance (NUJIA)*, *2*(1).

118. Kahneman, D. (2011). Thinking, fast and slow. Farrar, Straus and Giroux.

119. Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*(2), 263–292. https://doi.org/10.2307/1914185

120. Kanaan, A., Al-Hawamleh, A., Aloun, M., Alorfi, A., & Alrawashdeh, M. A. (2025). Fortifying organizational cyber resilience: An integrated framework for business continuity and growth amidst escalating threat landscapes. *International Journal of Computing and Digital Systems*, *17*(1), 1–14. https://journal.uob.edu.bh/items/ee82fb90-c52f-498c-a36f-1906941a4232

121. Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5766–5781. https://doi.org/10.1016/j.jksuci.2021.01.018

122. Kilani, Y. (2020). Cyber-security effect on organizational internal process: Mediating role of technological infrastructure. *Problems and Perspectives in Management*, *18*(1), 449–460. https://doi.org/10.21511/ppm.18(1).2020.39

123. Kline, R. B. (2016). Principles and practice of structural equation modeling (4th ed.). The Guilford Press.

124. Kosub, T. (2015). Components and challenges of integrated cyber risk management. *Zeitschrift für die gesamte Versicherungswissenschaft*, *104*(5), 615–634. https://doi.org/10.1007/s12297-015-0316-8

125. Kraus, S., Clauss, T., Breier, M., Gast, J., Zardini, A., & Tiberius, V. (2020). The economics of COVID-19: Initial empirical evidence on how family firms in five European countries cope with the corona crisis. *International Journal of Entrepreneurial Behavior & Research*, *26*(5), 1067–1092. https://doi.org/10.1108/IJEBR-04-2020-0214

126. Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk prediction for the critical infrastructure protection. *Neural Computing and Applications*, *34*(18), 15241–15271. https://doi.org/10.1007/s00521-022-06959-2

127. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105,* 102248. https://doi.org/10.1016/j.cose.2021.102248

128. Landoll, D. J. (2021). The security risk assessment handbook: A complete guide for performing security risk assessments (3rd ed.). *CRC Press*. https://doi.org/10.1201/9781003090441

129. Lee, M. (2023). Cyber threat intelligence. *John Wiley & Sons*. https://doi.org/10.1002/9781119861775

130. Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. *Human Resource Management Review*, *21*(3), 243–255. https://doi.org/10.1016/j.hrmr.2010.07.001

131. Li, J. H. (2018). Cyber security meets artificial intelligence: A survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462–1474. https://doi.org/10.1631/FITEE.1800573

132. Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

133. Lindström, J., Samuelsson, S., & Hägerfors, A. (2010). Business continuity planning methodology. *Disaster Prevention and Management, 19*(2), 243–255. https://doi.org/10.1108/09653561011038039

134. Linkov, I., & Kott, A. (2018). Fundamental concepts of cyber resilience: Introduction and overview. In A. Kott & I. Linkov (Eds.), *Cyber resilience of systems and networks* (pp. 1–25). Springer International Publishing. https://doi.org/10.1007/978-3-319-77492-3_1

135. Liu, Y., Guo, M., Han, Z., Gavurová, B., Bresciani, S., & Wang, T. (2024). Effects of digital orientation on organizational resilience: A dynamic capabilities perspective. *Journal of Manufacturing Technology Management*, *35*(2), 268–290. https://doi.org/10.1108/jmtm-06-2023-0224

136. Lovallo, D., & Sibony, O. (2010). The case for behavioral strategy. *McKinsey* Quarterly, March 2010. https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/the-case-for-behavioral-strategy

137. Malatji, M., Marnewick, A. L., & Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. *Information and Computer Security*, *30*(2), 255–279. https://doi.org/10.1108/ICS-06-2021-0091

138. Marotta, A., & McShane, M. (2018). Integrating a proactive technique into a holistic cyber risk management approach. *Risk Management and Insurance Review*, *21*(3), 435–452. https://doi.org/10.1111/rmir.12109

139. McDonald, R. P. (1999). Test theory: A unified treatment. Lawrence Erlbaum Associates. https://doi.org/10.4324/9781410601087

140. McManus, S., Seville, E., Vargo, J., & Brunsdon, D. (2008). Facilitated process for improving organizational resilience. *Natural Hazards Review*, *9*(2), 81–90. https://doi.org/10.1061/(ASCE)1527-6988(2008)9:2(81)

141. Mettler, T. (2011). Maturity assessment models: A design science research approach. *International Journal of Society Systems Science, 3*(1/2), 81–98. https://doi.org/10.1504/IJSSS.2011.038934

142. Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, *12,* 561011. https://doi.org/10.3389/fpsyg.2021.561011

143. Muhati, E., & Rawat, D. B. (2024). Data-driven network anomaly detection with cyber attack and defense visualization. *Journal of Cybersecurity and Privacy*, *4*(2), 241–263. https://doi.org/10.3390/jcp4020012

144. Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance. *Information Systems Frontiers*, *21*(5), 997–1018. https://doi.org/10.1007/s10796-017-9808-5

145. Nadji, B. (2024). Data security, integrity, and protection. In B. Nadji (Ed.), Data, security, and trust in smart cities (pp. 59–83). *Springer Nature Switzerland AG*. https://doi.org/10.1007/978-3-031-61117-9_4

146. Naicker, V., & Mafaiti, M. (2019). The establishment of collaboration in managing information security through multisourcing. *Computers & Security*, *80,* 224–237. https://doi.org/10.1016/j.cose.2018.10.005

147. National Association of Corporate Directors. (2023). Director's handbook on cyber-risk oversight. National Association of Corporate Directors. https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/nacd-directors-handbook-on-cyber-risk-oversight/

148. National Institute of Standards and Technology. (2010). Contingency planning guide for federal information systems (NIST Special Publication 800-34 Rev. 1). https://doi.org/10.6028/NIST.SP.800-34r1

149. National Institute of Standards and Technology. (2020). Zero trust architecture (NIST Special Publication 800-207). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207

150. National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST Cybersecurity White Paper 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

151. National Institute of Standards and Technology. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST Special Publication 800-61r3). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-61r3

152. Neri, M., Niccolini, F., & Virili, F. (2025). Organizational cyber resilience: Toward an integrative conceptual framework. *Management Review Quarterly*, *76*, 789–840. https://doi.org/10.1007/s11301-025-00496-7

153. Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. 2011 *First Workshop on Socio-Technical Aspects in Security and Trust (STAST 2011)* (pp. 60-68). IEEE. https://doi.org/10.1109/STAST.2011.6059257

154. Onwubiko, C. (2020). Focusing on the recovery aspects of cyber resilience *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (CyberSA, 2020) (pp. 1–13). IEEE. https://doi.org/10.1109/CyberSA49311.2020.9139685

155. Panteli, N., Nthubu, B. R., & Mersinas, K. (2025). Being responsible in cybersecurity: A multi-layered perspective. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-025-10588-0

156. Papadopoulos, T., Singh, S. P., Spanaki, K., Gunasekaran, A., & Dubey, R. (2022). Towards the next generation of manufacturing: Implications of big data and digitalization in the context of industry 4.0. *Production Planning & Control*, *33*(2–3), 101–104. https://doi.org/10.1080/09537287.2020.1810767

157. Paulk, M. (2002). Capability maturity model for software. *Encyclopedia of software engineering*. Wiley. https://doi.org/10.1002/0471028959.sof589

158. Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. *IEEE Security* & Privacy, *10*(3), 76–79. https://doi.org/10.1109/MSP.2012.73

159. Pavão, J., Bastardo, R., Carreira, D., & Rocha, N. P. (2023). Cyber Resilience, a Survey of Case Studies. *Procedia Computer Science*, *219,* 312–318. https://doi.org/10.1016/j.procs.2023.01.295

160. Peck, H. (2005). Drivers of supply chain vulnerability: An integrated framework. *International Journal of Physical Distribution & Logistics Management*, *35*(4), 210–232. https://doi.org/10.1108/09600030510599904

161. Pejić Bach, M., Krstić, Ž., Seljan, S., & Turulja, L. (2019). Text Mining for Big Data Analysis in Financial Sector: A Literature Review. *Sustainability*, *11*(5), 1277. https://doi.org/10.3390/su11051277

162. Pejić Bach, M., Topalović, A., Krstić, Ž., & Ivec, A. (2023). Predictive Maintenance in Industry 4.0 for the SMEs: A Decision Support System Case Study Using Open-Source Software. *Designs*, *7*(4), 98. https://doi.org/10.3390/designs7040098

163. Pendleton, M., Garcia-Lebron, R., Cho, J. H., & Xu, S. (2016). A survey on systems security metrics. *ACM Computing Surveys*, *49*(4), 1–35. https://doi.org/10.1145/3005714

164. Poeppelbuss, J., & Röglinger, M. (2011). What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management. *ECIS 2011 Proceedings*. 28. https://aisel.aisnet.org/ecis2011/28

165. Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

166. Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *The International Journal of Logistics Management, 20*(1), 124–143. https://doi.org/10.1108/09574090910954873

167. Porambage, P., & Liyanage, M. (2023). Security and privacy vision in 6G: A comprehensive guide. *John Wiley & Sons, Inc*. https://doi.org/10.1002/9781119875437.ch3

168. Porter, M. E. (1985). Competitive advantage: Creating and sustaining superior performance. *Free Press*.

169. Prakash, V. S., Murugesan, P., Poongothai, P., Shivakumar, B. N., Vijayakumar, P., & Shriidhar, P. J. (2024). Artificial Intelligence in Cybersecurity: Enhancing Automated Defense Mechanisms to Combat Sophisticated Cyber Threats and Guarantee Digital Resilience. *5th IEEE Global Conference for Advancement in Technology (GCAT),* pp. 1-6. https://doi.org/10.1109/GCAT62922.2024.10923968

170. Pratono, A. H. (2016). Strategic orientation and information technological turbulence: Contingency perspective in SMEs. *Business Process Management Journal*, *22*(2), 368–382. https://doi.org/10.1108/BPMJ-05-2015-0066

171. Proença, D., & Borbinha, J. (2016). Maturity models for information systems: A state of the art. *Procedia Computer Science*, *100,* 1042–1049. https://doi.org/10.1016/j.procs.2016.09.279

172. Putrus, R. (2019). The role of the CISO and the digital security landscape. *ISACA Journal*. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/the-role-of-the-ciso-and-the-digital-security-landscape

173. Queiroz, M. M., Ivanov, D., Dolgui, A., & Fosso Wamba, S. (2022). Impacts of epidemic outbreaks on supply chains: mapping a research agenda amid the COVID-19 pandemic through a structured literature review. *Annals of Operations Research*, *319,* 1159–1196. https://doi.org/10.1007/s10479-020-03685-7

174. Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cyber security maturity models: A systematic literature review. Information & Computer Security, *28*(4), 627–644. https://doi.org/10.1108/ICS-03-2019-0039

175. Radziwill, N. M., & Benton, M. C. (2017). Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management. *Software Quality Professional*, *19*(3). https://doi.org/10.48550/arXiv.1707.02653

176. Rajan, R., Rana, N. P., Parameswar, N., Dhir, S., Sushil, & Dwivedi, Y. K. (2021). Developing a modified total interpretive structural model (m-TISM) for organizational strategic cybersecurity management. *Technological Forecasting and Social Change*, *170,* 120872. https://doi.org/10.1016/j.techfore.2021.120872

177. Rajasekharaiah, K. M., Dule, C. S., & Sudarshan, E. (2020). Cyber security challenges and its emerging trends on latest technologies. *IOP Conference Series: Materials Science and Engineering*, *981,* 022062. https://doi.org/10.1088/1757-899X/981/2/022062

178. Rapaccini, M., Saccani, N., Kowalkowski, C., Paiola, M., & Adrodegari, F. (2020). Navigating disruptive crises through service-led growth: The impact of

COVID-19 on Italian manufacturing firms. *Industrial Marketing Management*, *88,* 225–237. https://doi.org/10.1016/j.indmarman.2020.05.017

179. Razzaq, K., & Shah, M. H. (2025). Advancing Cybersecurity Through Machine Learning: A Scientometric Analysis of Global Research Trends and Influential Contributions. *Journal of Cybersecurity and Privacy*, *5*(2), 12. https://doi.org/10.3390/jcp5020012

180. Rehan, S. (2023). AWS IoT with edge ML and cybersecurity: A hands-on approach. *Apress*. https://doi.org/10.1007/979-8-8688-0011-5_8

181. Rentsch, C., Sulger, P., & Finger, M. (2017). Major public enterprises in Switzerland. *ECONOMIA PUBBLICA* (2016/3). https://doi.org/10.3280/ep2016-003003

182. Rogers, E. M. (2003). Diffusion of innovations (5th ed.). *Free Press*.

183. Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

184. Rothrock, R. A., Kaplan, J., & Van der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*. https://sloanreview.mit.edu/article/the-boards-role-in-managing-cybersecurity-risks/

185. Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors*, *23*(16), 7273. https://doi.org/10.3390/s23167273

186. Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research*, *242*(1), 261–273. https://doi.org/10.1016/j.ejor.2014.09.055

187. Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2018). Building organizational resilience in the face of multiple disruptions. *International Journal of Production Economics*, *197,* 63–83. https://doi.org/10.1016/j.ijpe.2017.12.009

188. Salvi, A., Spagnoletti, P., & Noori, N. S. (2022). Cyber-resilience of critical cyber infrastructures: Integrating digital twins in the electric power ecosystem. *Computers & Security*, *112,* 102507. https://doi.org/10.1016/j.cose.2021.102507

189. Sánchez-García, I. D., Mejía, J., & San Feliu Gilabert, T. (2023). Cybersecurity risk assessment: A systematic mapping review, proposal, and validation. *Applied Sciences*, *13*(1), 395. https://doi.org/10.3390/app13010395

190. Sarker, I. H. (2021). CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. Internet of Things, *14,* 100393. https://doi.org/10.1016/j.iot.2021.100393

191. Sarker, I. H. (2022). AI-based modeling: Techniques, applications, and research issues towards automation, intelligent, and smart systems. *SN Computer Science*, *3*(2), 158. https://doi.org/10.1007/s42979-022-01043-x

192. Securities and Exchange Commission. (2023). Cybersecurity risk management, strategy, governance, and incident disclosure. Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

193. Seetharaman, P. (2020). Business models shifts: Impact of Covid-19. International *Journal of Information Management, 54,* 102173. https://doi.org/10.1016/j.ijinfomgt.2020.102173

194. Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & Security*, *97,* 101996. https://doi.org/10.1016/j.cose.2020.101996

195. Shahim, A. (2021). Security of the digital transformation. *Computers & Security*, *108,* 102345. https://doi.org/10.1016/j.cose.2021.102345

196. Sheffi, Y. (2005). The resilient enterprise: Overcoming vulnerability for competitive advantage. *MIT Press*. https://mitpress.mit.edu/9780262693493/the-resilient-enterprise/

197. Snedaker, S. (2013). Business continuity and disaster recovery planning for IT professionals. *Newnes*.

198. Sonnenschein, R., Loske, A., & Buxmann, P. (2017). The Role of Top Managers' IT Security Awareness in Organizational IT Security Management. *ICIS*

2017 Proceedings, 13. Association for Information Systems (AIS) eLibrary. https://aisel.aisnet.org/icis2017/Security/Presentations/13/

199. Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, *34*(3), 503–522. https://doi.org/10.2307/25750689

200. Spremić, M. (2013). Holistic approach to governing information system security. *Lecture Notes in Engineering and Computer Science, 2*, 1242–1247.

201. Spremić, M., & Šimunic, A. (2018). Cyber security challenges in digital economy. *Proceedings of the World Congress on Engineering, 1*, 341–346.

202. Spremić, M., Turulja, L., & Bajgorić, N. (2018). Two approaches in assessing business continuity management attitudes in the organizational context. In N. Bajgorić (Ed.), *Always-on enterprise information systems for modern organizations* (pp. 159–183). IGI Global.

203. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1–11. https://doi.org/10.1016/j.jnca.2010.07.006

204. Swiss Federal Statistical Office. (2023). Structural statistics of enterprises (STATENT). https://www.bfs.admin.ch/bfs/en/home/statistics/industry-services/stagre.html

205. Swiss Financial Market Supervisory Authority (FINMA). (2022). Circular 2023/1: Operational risks and resilience – banks. finma-rs-2023-01-20221207.pdf

206. Swiss Financial Market Supervisory Authority (FINMA). (2024). FINMA risk monitor 2024: Principal risks for the financial sector. FINMA Risk Monitor 2024: Principal risks for the financial sector and uncertainties due to geopolitical tensions | FINMA

207. Tan, W., Guo, B., & Zhang, Q. (2025). Cybersecurity governance and corporate market value: Perspectives from investor trust and supply chain trust. *Pacific-Basin Finance Journal, 90,* 102646. https://doi.org/10.1016/j.pacfin.2024.102646

208. Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic management journal*, *18*(7), 509-533.https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z

209. The Open Group. (2022). The TOGAF Standard, 10th Edition. https://www.opengroup.org/togaf

210. Thompson, E. C. (2018). Cybersecurity incident response: How to contain, eradicate, and recover from incidents. *Apress*.

211. Trim, P. R. J., & Upton, D. (2013). Cyber Security Culture: Counteracting Cyber Threats Through Organizational Learning and Training. *Routledge*. https://doi.org/10.4324/9781315575681

212. Tushman, M. L., & Anderson, P. (1986). Technological discontinuities and organizational environments. *Administrative Science Quarterly*, 31(3), 439–465. https://doi.org/10.2307/2392832

213. U.S. Congress. (2002a). Federal Information Security Management Act of 2002 (FISMA). Public Law 107-347. https://www.congress.gov/bill/107th-congress/house-bill/3844/text

214. U.S. Congress. (2002b). Sarbanes-Oxley Act of 2002. Public Law 107-204.

215. U.S. Department of Defense. (2022). *Cybersecurity Maturity Model Certification (CMMC) 2.0 program*. https://dodcio.defense.gov/CMMC/

216. U.S. Department of Homeland Security. (2024). *DHS strategic plan: Fiscal years 2023–2027*. https://www.dhs.gov/sites/default/files/2024-11/24_1119_plcy_dhs-strategic-plan-fy23-27.pdf

217. Van Laak, D. (2004). Technological infrastructure, concepts and consequences. *Icon*, 53-64.

218. Verma, P., Newe, T., O'Mahony, G. D., Brennan, D., & O'Shea, D. (2025). Toward a Unified Understanding of Cyber Resilience: Concepts, Strategies, and Future Directions. *IEEE Access*, *13,* 49945–49965. https://doi.org/10.1109/ACCESS.2025.3551887

219. Wallace, M., & Webber, L. (2017). The disaster recovery handbook: A step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets (3rd ed.). *AMACOM*.

220. Yamin, M. M., & Katt, B. (2022). Modeling and executing cyber security exercise scenarios in cyber ranges. *Computers & Security*, *116,* 102635. https://doi.org/10.1016/j.cose.2022.102635

221. Yan, F., Li, N., Iliyasu, A. M., Salama, A. S., & Hirota, K. (2023). Insights into security and privacy issues in smart healthcare systems based on medical images. *Journal of Information Security and Applications*, *78*, 103621. https://doi.org/10.1016/j.jisa.2023.103621

222. Yulianto, E., Ali, Q. S. A., Hanafiah, M. H., Wiyata, W., & Salamah, S. N. (2025). Strengthening resilience and performance through business continuity management: insights from central java tour operators. *Quality & Quantity*, 1-27. https://doi.org/10.1007/s11135-025-02285-6

223. Zsidisin, G. A., Melnyk, S. A., & Ragatz, G. L. (2005). An institutional theory perspective of business continuity planning for purchasing and supply management. *International journal of production research*, *43*(16), 3401-3420. https://doi.org/10.1080/00207540500095613

Annex 1. Questionnaire: Benchmark controls

SECTION 1: RESILIENCE (R)

1. **Our organization has robust business continuity plans in place to manage the impact of cybersecurity incidents and keep our critical activities functioning.**

Benchmark Controls:

- Business continuity architecture - 100% of critical business functions have documented backup systems, alternative processes and recovery procedures, with RTO (Recovery Time Objective) and RPO (Recovery Point Objective) that are determined by the business impact analysis based on the organizational criticality and not fixed timeframes (International Organization for Standardization, 2019; Sahebjamnia et al., 2015; Federal Office for National Economic Supply, 2023).
- Incident containment - All cyber incidents are contained according to documented incident response procedures with defined containment strategies appropriate to the incident type and severity, following incident response guidelines for effective containment, eradication, and recovery (Ahmad et al., 2020; Thompson, 2018).
- Operational resilience - Organization maintains documented service delivery targets during disruptions based on business impact analysis and regulatory requirements, with evidence of successful resilience testing and validation (International Organization for Standardization, 2019; FINMA, 2022).

2. **Our organization demonstrates rapid adaptation of cybersecurity strategies and processes in response to changes in the threat landscape**.

Benchmark Controls:

- Adaptive security architecture - Security controls and policies are reviewed and adjusted according to threat intelligence and risk assessments, with documented change control processes in place to allow for rapid adaptation to new threats (National Institute of Standards and Technology, 2024; Ahmad et al., 2020).

- Threat response agility - New cyberthreat defenses are developed and implemented based on organizational dynamic capabilities and threat intelligence analysis, with documented evidence of successful threat mitigation (Ahmad et al., 2020; CISA, 2024).
- Strategic flexibility – Cybersecurity strategies are regularly reviewed and updated based on changing business and threat environments, with senior leadership approval of significant strategic changes (Ahmad et al., 2020; National Institute of Standards and Technology, 2024).

3. **Our organization systematically learns from past cybersecurity incidents and integrates lessons learned into improved security practices.**

Benchmark Controls:

- Post-incident debriefing – All cybersecurity incidents have a written post-incident review debrief to include root cause analysis, and lessons learned documentation in accordance with incident response recommendations (Ahmad et al., 2020; Thompson, 2018).
- Integration learning – All lessons acquired are integrated in revised policy, procedures, and training programs within documented timescales, and evidence of implementation of the revisions is documented (ISO, 2023; Ahmad et al., 2020).
- Continual improvement - Security posture improvements can be measured via tracking metrics that reflect a decrease in the rate of similar incident recurrence and also an increase in detection capabilities (Lengnick-Hall et al., 2011; Pendleton et al., 2016).

SECTION 2: CYBER SECURITY RISK MATURITY (CSRM)

1. **Our organization has established procedures in respect of the identification and assessment of cybersecurity risks.**

Benchmark Controls:

- Risk identification methodology – All critical business areas and critical third-party providers undergo structured cybersecurity risk discovery and categorization at least

annually and following significant changes in the organization's risk profile, threat environment, or regulatory requirements, aligned with the Identify function of the NIST Cybersecurity Framework 2.0 (National Institute of Standards and Technology, 2024; International Organization for Standardization, 2022a).

- Threat intelligence incorporation - External threat intelligence is systematically integrated into risk assessment procedures through documented processes, with impact analysis conducted for relevant threats according to organizational threat intelligence frameworks (Saeed et al., 2023; Kure et al., 2022).
- Comprehensive risk register – An aggregated inventory of all identified risks is kept in a central repository and is updated regularly, reviewed, and validated periodically to ensure comprehensive coverage of all critical business domains (National Institute of Standards and Technology, 2024; COSO, 2017).
- Business process integration - Cybersecurity risk management framework is strategically aligned with business process objectives and acceptable impact thresholds, incorporating formal business impact analysis and documented risk tolerance levels (International Organization for Standardization, 2022a; COSO, 2017).

2. **Our organization implements effective cybersecurity risk mitigation and control measures.**

Benchmark Controls:

- Control effectiveness – Security controls achieve risk reduction of targeted threats in a measurable way through evidence-based documentation and ongoing evaluation (aligned with NIST CSF 2.0 and ISO/IEC 27005:2022 Annex A) (National Institute of Standards and Technology, 2024; International Organization for Standardization, 2022a; FAIR Institute, 2024).
- Defense-in-depth architecture - Comprehensive security architecture incorporates preventive, detective, and corrective controls across critical assets with documented redundancy for essential security functions (National Institute of Standards and Technology, 2024; International Organization for Standardization, 2022a).
- Risk treatment optimization – Cost-benefit analysis are conducted for primary risk mitigation measures using defined risk quantification methodologies, with documented

justification of the expected return on investment (Freund & Jones, 2014; ISACA, 2022).

3. **Our organization has comprehensive monitoring of cyber risks with reporting to leadership.**

Benchmark Controls:

- Continuous monitoring - Security control effectiveness and risk level are monitored continuously or near-real time using automated tools or systems, with mechanisms in place to inform of the occurrence of critical control failures (National Institute of Standards and Technology, 2024; FINMA, 2022).
- Risk metrics and KPIs – Defined quantitative cybersecurity risk metrics are continuously monitored, analyzed for trends, and reported to executive leadership regularly (Kure et al., 2022; International Organization for Standardization, 2016).
- Executive reporting – The risk function reports on the status of risks to top leadership regularly and advises on next steps, including material on a risk dashboard and risk training needs assessment prepared for management as and where needed (Burch et al., 2024; European Parliament and Council of the European Union, 2022a; National Association of Corporate Directors, 2023).

SECTION 3: TECHNOLOGICAL INFRASTRUCTURE (TI)

1. **Our organization maintains a robust and secure technological infrastructure.**

Benchmark Controls:

- Infrastructure resilience – Critical systems have appropriate redundancy configuration with automated failover capabilities, achieving uptime levels consistent with business requirements based on Business Impact Analysis, with disaster recovery infrastructure tested regularly (International Organization for Standardization, 2019; The Open Group, 2022).
- Security architecture - Technology components have security controls embedded into them across the IT environment throughout their lifecycle, with consideration to secure-

by-design and security architecture frameworks (Geismann et al., 2018; National Institute of Standards and Technology, 2024).

- Stress testing – During attack simulations or periods of high demand, our infrastructure remains operational and secured, and stress testing is documented and reviewed regularly (CISA, 2023a; Yamin & Katt, 2022).

2. Our organization operates integrated and scalable technology systems.

Benchmark Controls:

- System integration - Technology platforms and security tools share data through documented integration frameworks with centralized logging and monitoring capabilities, providing comprehensive visibility across the enterprise (The Open Group, 2022; Aldea et al., 2023).
- Scalability architecture - Technology infrastructure scales to accommodate business growth without security degradation, with cloud-native principles implemented where appropriate and documented scalability assessments (Aldea et al., 2023; National Institute of Standards and Technology, 2024; Lee, 2023).
- Unified security management – Security management integrates technology, ensuring security coverage of technology environments through central visibility, control, and policy enforcement (National Institute of Standards and Technology, 2024; Nadji, 2024).

3. Our organization deploys advanced cybersecurity tools and technologies.

Benchmark Controls:

- Next generation security technology – Modern security technologies (e.g., AI-driven threat detection, zero-trust architecture, advanced analytics) are implemented across infrastructure with documented effectiveness metrics, and regular capability reviews are conducted (National Institute of Standards and Technology, 2024; Malatji et al., 2022).
- Threat detection features – Threat detection capabilities are measured through Mean Time to Detect (MTTD), detection accuracy, and response time to threats, with metrics reviewed regularly across relevant threat categories (National Institute of Standards and

Technology, 2024; Cybersecurity and Infrastructure Security Agency, 2023a; Lee, 2023).

- Adoption of innovation - The adoption of innovative cybersecurity technologies is frequently evaluated and implemented based on evidence when it contributes to security gains according to documented evaluation criteria and implementation procedures (Rogers, 2003; Prakash et al., 2024).

SECTION 4: CYBER SECURITY RESOURCES AND CAPABILITIES (CSRC)

1. **Our organization maintains skilled cybersecurity employees.**

Benchmark Controls:

- Talent management – Cybersecurity team demonstrates effective talent retention through documented HR metrics and succession planning, maintaining staffing levels appropriate for the organizational risk profile (ISACA, 2022; (ISC)², 2023).
- Leadership qualifications – Senior cybersecurity leadership positions are filled by qualified professionals with appropriate certifications (Certified Information Systems Security Professional, Certified Information Security Manager, or equivalent) and relevant experience commensurate with organizational complexity (ISACA, 2022; (ISC)², 2023).
- Skills development – Formal professional learning activities with appropriate training budgets and well-planned curricula (e.g., tailored to requirements) specified in NIST NICE Cybersecurity Workforce Framework competencies (Paulsen et al., 2012; Hatzivasilis et al., 2020).

2. **Our organization maintains effective cybersecurity technology and tool capabilities.**

Benchmark Controls:

- Advanced threat detection – Security solutions demonstrate effective threat detection and response capabilities through documented performance metrics and independent

validation aligned with recognized industry evaluation frameworks (National Institute of Standards and Technology, 2024).

- Operational intelligence - Security tools produce concise, prioritized alerts that elicit effective responses according to a documented alert management process, with reasonable false positive rates and response time figures (National Institute of Standards and Technology, 2024; Razzaq & Shah, 2025).
- Technology lifecycle management – Formal processes are in place to review and patch security technologies and to maintain, replace, and retire software and hardware commensurate with risk (International Organization for Standardization, 2022b; National Institute of Standards and Technology, 2024).

3. **Our organization allocates cybersecurity budget and resources effectively.**

Benchmark Controls:

- Appropriate funding – Cybersecurity budget allocation is reviewed against the organization's risk profile and supported by documented risk-based investment analysis (Gordon et al., 2016; FAIR Institute, 2024).
- Risk-based investment – Cybersecurity investments are supported by quantitative business risk analysis and documented business cases using recognized risk quantification methodologies with ROI calculations (FAIR Institute, 2024; Freund & Jones, 2014).
- Flexible funding mechanisms - Emergency cybersecurity funding mechanisms enable rapid response to urgent threats or vulnerabilities through documented escalation procedures, considering organizational dynamic capabilities (National Institute of Standards and Technology, 2024).

SECTION 5: CYBER SECURITY AWARENESS (CSA)

1. **Our organization provides employees with effective cybersecurity knowledge and understanding.**

Benchmark Controls:

- Comprehensive programs – Employees receive regular cybersecurity awareness programs, with high-risk positions receiving enhanced targeted training based on current threat vectors (Hatzivasilis et al., 2020; National Institute of Standards and Technology, 2024).
- Effectiveness monitoring - The effectiveness is monitored by simulated phishing exercises and other assessments, click-through and reporting rates tracked over time against an organization-specific baseline and visible behavior change (Chaudhary et al., 2022; Moustafa et al., 2021).
- Security culture assessment – Periodic assessment of cybersecurity culture through validated survey instruments and behavioral indicators, with documented improvement plans based on assessment results (Alshaikh, 2020; Da Veiga & Martins, 2015).

2. **Our organization fosters a strong cybersecurity culture and employee engagement.**

Benchmark Controls:

- Cultural integration – Cybersecurity responsibilities are embedded in job role descriptions and annual performance reviews of relevant staff, with security-related KPIs added for employees dealing with sensitive information (Da Veiga & Martins, 2015; Alshaikh, 2020).
- Incident reporting culture - Staff voluntarily report security incidents and near misses and are not penalized for reporting. Evidence suggests a positive reporting culture and timely incident notification processes (ISO, 2023; Ahmad et al., 2020).
- Leadership commitment – Senior management shows a visible commitment to cybersecurity with frequent communications, realistic budgeting, and strong involvement in security efforts and drills (Rothrock et al., 2018; Arbanas et al., 2021).

3. **Our organization's employees demonstrate awareness of cybersecurity threats and best practices in their daily work.**

Benchmark Controls:

- Behavioral metrics - User-reported phishing emails, adherence to clean desk policies, and safe data handling practices are tracked and show positive trends (Arbanas et al., 2021).

- Security policy adherence - Audits and observations confirm that employees are following key security policies (e.g., password policies, acceptable use policies) (He & Zhang, 2019).
- Employee feedback - Surveys and interviews indicate that employees understand their role in protecting the organization from cyber threats (Alshaikh, 2020).

SECTION 6: CYBER SECURITY TRAINING (CST)

1. **Our organization has comprehensive and effective cybersecurity programs.**

Benchmark Controls:

- Role-based training curriculum - Content is designed for the general workforce, privileged users, and software developers based on NIST NICE Framework principles to offer a broad spectrum of role-based training across the organization (Paulsen et al., 2012; Chowdhury et al., 2022).
- Regularity and frequency of training – Employees are trained at induction and given regular refresher training during their employment, providing consistent base knowledge across the organization (Paulsen et al., 2012; Hatzivasilis et al., 2020).
- Risk coverage – Training programs cover key organization information security risks such as phishing, social engineering, and handling information securely as mandated by ISO/IEC 27001:2022 (International Organization for Standardization, 2022b; Hatzivasilis et al., 2020).

2. **Our organization provides effective cybersecurity skill development and competency building.**

Benchmark Controls:

- Specialized technical training – Dedicated advanced training programs support technical staff with appropriate budget allocation and alignment to specific NIST NICE Framework Work Roles (Paulsen et al., 2012; Chowdhury et al., 2022).

- Simulation-based learning – Incident Response team conducts simulated scenarios and table-top exercises regularly to stay prepared and trial response capabilities (Hatzivasilis et al., 2020; National Institute of Standards and Technology, 2024).
- Competency assessment – Formal mechanisms are used to measure and monitor cybersecurity proficiency, as compared to established standards with periodic audits and documented corrective actions (Paulsen et al., 2012; Chowdhury et al., 2022).

3. **Our organization's cybersecurity training program is continuously improved based on formal assessments.**

Benchmark Controls:

- Comprehensive measures of effectiveness – Measurement for effectiveness of training includes knowledge retention, change in behavior indicators, and applications in real-life situations as evidence of improvement in security posture (Chowdhury et al., 2022; Arbanas et al., 2021).
- Integration of feedback - The organization maintains a system for gathering feedback from staff that enables continuous improvement, with evidence that the improvements made as a result of the feedback were tracked and implemented promptly (Deming, 2000; Chowdhury et al., 2022).
- Program evolution – Training programs are updated regularly to reflect the latest threat intelligence and lessons learned from incidents (Hatzivasilis et al., 2020).

SECTION 7: CYBER SECURITY ALLIANCE & COLLABORATION (CSAC)

1. **Our organization demonstrates effective cybersecurity partnerships and development.**

Benchmark Controls:

- Industry leadership and participation – Organization maintains active leadership or contributing roles in relevant industry Information Sharing and Analysis Centers (ISACs) for Swiss operations, with documented participation and engagement

(European Union Agency for Network and Information Security, 2018; Federal Council, 2023).

- Government collaboration – Organization has established formal documented relationships with regional and national cybersecurity organizations (i.e., the Swiss Federal Office for Cybersecurity [BACS; formerly NCSC]) for regular engagement activities and information sharing (Federal Council, 2023).
- Academic partnerships – Organization maintains active cooperation with academic institutions in Switzerland and/or neighboring countries in cybersecurity R&D and education, with documented collaborative activities and knowledge exchange (European Union Agency for Network and Information Security, 2018; Federal Council, 2023; CISA, 2023a).

2. **Our organization exhibits effective cybersecurity information sharing and intelligence collaboration.**

Benchmark Controls:

- Threat information sharing – Our organization is involved in bi-directional threat information sharing with other industry entities and government entities through sharing agreements and documented procedures for sharing information (Fransen et al., 2015; Saeed et al., 2023).
- Cross-border collaboration – Adequate information-sharing relationships are established with foreign cybersecurity authorities respecting Swiss neutrality and maintaining data sovereignty (Federal Council, 2023; Federal Assembly of the Swiss Confederation, 2023).
- Supply chain security collaboration – Organization is actively involved in supply chain security programs and information sharing in partnership with key suppliers and partners that meet NIS2 supply chain requirements where applicable (European Commission, 2023; Christopher & Peck, 2004).

3. **Our organization participates actively in industry-wide cybersecurity initiatives.**

Benchmark Controls:

- Industry collaboration - Organization actively engages in cybersecurity knowledge sharing activities (conference, working group, research collaboration) and shows evidence of its contribution to the cybersecurity community (Naicker & Mafaiti, 2019; economiesuisse, 2023).
- Collective defense participation - Organization participates in collective defense services (e.g., Computer Emergency Response Team [CERT]/Computer Security Incident Response Team, threat intelligence sharing, system log collection) (economiesuisse, 2023; He et al., 2017).
- Standards development – Contribution to cybersecurity standards development as well as best practice sharing within industry associations and professional organizations (Federal Council, 2023).

SECTION 8: CYBER SECURITY TOP MANAGEMENT SUPPORT (CSTMS)

1. **Our organization's top management demonstrates a strong commitment to cybersecurity and effective resource allocation.**

Benchmark Controls:

- Strategic alignment – Security personnel conduct an annual review of the cybersecurity strategy to ensure alignment with business goals, with formal board approval and documented alignment-assessment methods, in line with the NIST CSF 2.0 implementation examples for GV.RR-01 (National Institute of Standards and Technology, 2024; National Association of Corporate Directors, 2023).
- Budget protection – Cybersecurity budget is protected during times of cost reduction with documented justification processes from the senior management, ensuring adequate funding for critical security functions (Deloitte, 2023).
- Leadership advocacy - Senior leaders are observed to serve as public and internal advocates of cybersecurity as a business enabler, evidenced by documented communications and stakeholders' engagement activities (National Association of Corporate Directors, 2023; Rothrock et al., 2018).

2. **Our organization's leadership exhibits effective cybersecurity governance and oversight.**

Benchmark Controls:

- Board cybersecurity expertise – Board-level risk committee includes members with technical cybersecurity background and relevant certifications (Certified Information Systems Security Professional, Certified Information Security Manager, or equivalent) or sufficient professional expertise to make informed cybersecurity risk assessments (Rothrock et al., 2018; National Association of Corporate Directors, 2023).
- CISO governance model – The CISO holds a C-suite or senior-level position with established reporting lines and regular access to the board or risk committee on key cybersecurity issues (Putrus, 2019; Gartner, 2023).
- Performance accountability – Cybersecurity performance factors are integrated into senior executive accountability frameworks through documented KPIs and performance measurement systems (International Organization for Standardization, 2016; Gartner, 2023).

3. **Our organization's top management ensures accountability for cybersecurity performance.**

Benchmark Controls:

- Metrics-based oversight – Cybersecurity performance is regularly reported to the board through a structured, metrics-based dashboard indicating the complete list of KPIs and Key Risk Indicators (International Organization for Standardization, 2016; National Association of Corporate Directors, 2023).
- Business unit accountability – A formal governance model to hold business unit leaders accountable for cybersecurity risks in their area of responsibility, with documented roles and responsibilities, and measured periodically (Putrus, 2019; National Institute of Standards and Technology, 2024).
- Accountability, including authority and resources - Cybersecurity accountability requires more than clearly defined roles and responsibilities; it also requires the appropriate delegation of authority and sufficient resources to enable effective cybersecurity performance, supported by documentation demonstrating adequate

empowerment and resources (European Parliament and Council of the European Union, 2022a; National Institute of Standards and Technology, 2024).

SECTION 9: CYBERSECURITY TOP MANAGEMENT RISK PERCEPTION (CSTMRP)

1. **Our organization's top management demonstrates an accurate understanding of cybersecurity risk assessment.**

Benchmark Controls:

- Cyber risk perception alignment – The leadership perception of the top cyber risks is aligned with the technical assessments through the documented risk communication process and periodic alignment reviews (COSO, 2017; Lovallo & Sibony, 2010).
- Systems thinking – Leadership understands the risks of interconnectivity and cascade of risks across the organization and into the supply chain by documented risk scenario analysis and strategic planning (International Organization for Standardization, 2018; Assenza et al., 2024).
- Decision-making processes – Structured decision-making protocols and cognitive bias mitigation strategies are part of cybersecurity risk assessment processes for main risk assessments (Kahneman, 2011; Lovallo & Sibony, 2010).

2. **Our organization's senior leadership exhibits effective cybersecurity threat awareness and intelligence utilization.**

Benchmark Controls:

- Regular threat briefings – Senior leadership receives structured briefings on the current cyber threat landscape with specific organizational impact analysis and documented action items (COSO, 2017; Dal Cin et al., 2025).
- Strategic intelligence integration – Threat intelligence directly impacts strategic business decisions, and there are written instances of intelligence-based decision-

making (i.e., market entry, product feature development, partnerships) (Dal Cin et al., 2025; Saeed et al., 2023).

- External engagement – Senior leaders engage in external cybersecurity events to keep abreast of emerging threats and the latest in industry best practice (Deloitte, 2023; Dal Cin et al., 2025).

3. **Our organization's executives make decisions with a comprehensive awareness of cyber risks.**

Benchmark Controls:

- Risk-informed decision making – Business decisions include documented cyber risk assessment and analysis, with formal risk versus return evaluation processes for strategic initiatives (Gordon & Loeb, 2002; COSO, 2017).
- Risk-based project governance – There are also documented instances where projects were altered or ceased because the cyber risk was deemed unacceptable, demonstrating mature risk-informed decision making (COSO, 2017; National Institute of Standards and Technology, 2024).
- Scenario planning – Documented scenario planning exercises that consider multiple cyber risk scenarios and their potential business impacts, including worst-case scenario analysis (National Association of Corporate Directors, 2023).

SECTION 10: MARKET TURBULENCE

1. **Our organization operates in an unpredictable, rapidly changing market.**

Benchmark Controls:

- Market volatility monitoring - Regular monitoring of market volatility indicators, i.e., customer demand fluctuations, competitive forces, and regulatory changes, along with market analysis and development of strategic response plans (Liu et al., 2024; Durst et al., 2024).

- Competitive landscape tracking - Systematic monitoring of competitive threats, market disruptions, and industry transformation that includes documented competitive intelligence and strategic positioning analysis (Porter, 1985; Pratono, 2016).
- Regulatory observatory – Continuous tracking of regulatory changes and compliance requirements across relevant jurisdictions with documented regulatory impact assessment and adaptation planning (European Parliament and Council of the European Union, 2016; Federal Assembly of the Swiss Confederation, 2023).

2. **Our organization faces frequent and intense competitive threats and market disruptions.**

Benchmark Controls:

- Competitive threat assessment - Ongoing competitive-threat analysis, including new market entrants, disruptive technologies, and customer-preference changes, with documented threat assessment and response plans (Porter, 1985; Pratono, 2016).
- Market disruption preparedness – Preparedness for market disruptions via scenario planning, contingency planning, and adaptive strategy formation in conjunction with documented disruption response capabilities (National Association of Corporate Directors, 2023).
- Innovation pressure control - Pressures to innovate and adopt new technologies in order to remain competitive are managed through a documented innovation strategy and implementation plan (Rogers, 2003; Christensen, 1997).

3. **Our organization experiences external stakeholder pressure and conflicting demands (e.g., from regulators vs. customers).**

Benchmark Controls:

- Stakeholder pressure – Our organization identifies relevant internal and external stakeholders and systematically considers their cybersecurity-related needs and expectations in its risk management and engagement activities (Kure et al., 2022; National Institute of Standards and Technology, 2024)

- Resolution of conflicting demands – Identifying potential conflicts among stakeholder interests and balancing and reconciling competing stakeholder needs in organizational decision-making (Freeman et al., 2020; Kure et al., 2022).
- Balance of regulatory compliance - The relative balance of regulatory requirements and business objectives, with documented compliance strategy and the risk-benefit analysis (FINMA, 2022; Federal Council, 2023).

SECTION 11: TECHNOLOGICAL TURBULENCE (TT)

1. **Our organization operates in a rapidly evolving and unpredictable technological environment.**

Benchmark Controls:

- Technology evolution monitoring - Trend tracking of new technologies is monitored systematically and relevant to the organization, in combination with technology forecasting, the development of R&D projects, and strategic planning (National Institute of Standards and Technology, 2024; Christensen, 1997).
- Management of digital transformation pressure - Managing digital transformation pressure and the necessity of technology adoption with a documented transformation strategy, including implementation roadmaps (Liu et al., 2024; Rogers, 2003).
- Innovation cycle adjustment - Accelerated innovation cycles and technology refresh demands are managed through documented innovation management and technology lifecycle planning (Rogers, 2003; Christensen, 1997).

2. **Our organization experiences complexity in integrating and managing multiple emerging technologies.**

Benchmark Controls:

- Technology integration complexity management - Ability to manage technology integration complexity, including system interoperability, data integration, and architectural coherence with documented integration frameworks and governance (The Open Group, 2022; Papadopoulos et al., 2022).

- Technology assimilation – Systematized assimilation of emerging technology, including assessment and pilot programs, has been scaled up, with documented technology assimilation processes (Rogers, 2003; Tushman & Anderson, 1986).
- Multi-technology integration - Integration of multi-technology platforms and initiatives is guided by strategic fit and integration efficiency, supported by cataloged technology portfolio management (Teece et al., 1997; Christensen, 1997).

3. **Our organization faces pressure to rapidly adopt new technologies to remain competitive.**

Benchmark Controls:

- Competitive technology pressure management - Balancing the competitive pressure for rapid technological adoption against systemic security and operational management requirements via a documented adoption strategy and risk mitigation assessment (Porter, 1985; Rogers, 2003).
- Technology adoption speed optimization - Optimizing the technology adoption speed to achieve a strategic balance among competitive advantage, implementation risks, and resource constraints, supported by a documented acceleration framework (Rogers, 2003; Liu et al., 2024).
- Innovation security balance - Technology-adoption decisions balance innovation requirements and cybersecurity considerations through documented security-by-design principles and risk-management strategies (Geismann et al., 2018; European Union, 2024).

CURRICULUM VITAE

Personal Information:

- **Name:** Martina Schmucki
- **Date of Birth:** September 26, 1979

Education:

- **Master in Business Administration:** University of Zagreb, Zagreb (CRO)
- **Master of Science (Environment and Resource Management):** Vrije Universiteit, Amsterdam (NL)

Professional Experience:

- 2023-present; **Security Consultant & Project Manager (Glencore plc), Netcloud AG, Switzerland**
- 2022-2023; **Sales Manager, GEOINFO Group, Switzerland**
- 2021-2022; **Key Account Manager, Indasys, Germany**
- 2017-2022; **Lecturer, United International Business Schools, Switzerland**
- 2015-2018; **Teacher, International School of Schaffhausen, Switzerland**

Key Projects and Certifications:

- **CISSP:** Certified Information Systems Security Professional.
- **PRINCE2**: Project Management certification.
- **Cybersecurity Consulting:** Governance and Awareness on operational and strategic levels.
- **International Project Management:** Leadership of international projects across Switzerland, the EU, and globally.