applied sciences

MDPI

Systematic Review

Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards

Ali Aghazadeh Ardebili [1,2], Marianna Lezzi [1,*] and Mahdad Pourmadadkar [1]

[1] Department of Engineering for Innovation, University of Salento, 73100 Lecce, Italy; ali.a.ardebili@unisalento.it (A.A.A.); mahdad.pourmadadkar@unisalento.it (M.P.)
[2] Department of Research and Development, HSPI SpA-Roma, 00185 Rome, Italy
* Correspondence: marianna.lezzi@unisalento.it

Abstract: As future infrastructures increasingly rely on digital systems, their exposure to cyber threats has grown significantly. The complex and hyper-connected nature of these systems presents challenges for enhancing cyber resilience against adverse conditions, stresses, attacks, or compromises on cybersecurity resources. Integrating risk assessment with cyber resilience allows for adaptive approaches that can effectively safeguard critical infrastructures (CIs) against evolving cyber risks. However, the wide range of methods, frameworks, and standards—some overlapping and others inadequately addressed in the literature—complicates the selection of an appropriate approach to cyber risk assessment for cyber resilience. To investigate this integration, this study conducts a systematic literature review (SLR) of relevant methodologies, standards, and regulations. After conducting the initial screening of 173 publications on risk assessment and cyber resilience, 40 papers were included for thorough review. The findings highlight risk assessment methods, standards, and guidelines used for cyber resilience and provide an overview of relevant regulations that strengthen cyber resilience through risk assessment practices. The results of this paper will offer cybersecurity researchers and decision-makers an illuminated understanding of how risk assessment enhances cyber resilience by extracting risk assessment best practices in the literature supported by relevant standards and regulations.

Keywords: cyber resilience; risk assessment; critical infrastructures

Citation: Aghazadeh Ardebili, A.; Lezzi, M.; Pourmadadkar, M. Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards. *Appl. Sci.* **2024**, *14*, 11807. https://doi.org/10.3390/app142411807

Academic Editors: David Megías and Reiner Creutzburg

Received: 27 September 2024
Revised: 4 December 2024
Accepted: 12 December 2024
Published: 17 December 2024

1. Introduction

The modern world has become increasingly interconnected thanks to recent disruptive advancements in information and communication technology (ICT). The complexity of systems in the digitalized era and the cyber–physical nature of emerging technologies have raised new issues regarding their safe and secure operation [1]. These issues become even more serious in the case of CIs, in which cyber incidents may have severe and vital consequences [2,3]. CIs are complex systems that provide a vital service to society, consisting of essential systems such as energy, transportation, and healthcare [4,5].

The complex and hyper-connected nature of these systems have made cyber resilience an ever-growing concern in CIs [6] and a crucial challenge to address [7]; it revolves around maintaining operational reliability to protect digitally interconnected systems from the negative impacts of cyber incidents [8].

Cyber resilience is defined in different ways depending on the application domain. Several meanings may be inferred from the term 'cyber resilience', ranging from just a by-product of security practices to a set of distinct processes that lead to the adaptive capacity of the system [8]. According to Alhidaifi et al. [9], cyber resilience is the system's ability to 'roll back' and resume normal operation once an incident disrupts it. From another perspective, cyber resilience may be inferred as dealing with 'unknown unknowns', i.e., it involves readiness for 'unpredictable, unforeseeable, and unexpected' cyber threats [10].

For the purpose of this study, cyber resilience refers to the ability of a system to prepare for, absorb, recover from, and adapt to adverse effects, particularly those arising from cyber-attacks [11]. It involves implementing reactive techniques such as alternative operations and dynamic feature composition to build resilient systems [12]. The primary objective of cyber resilience is to ensure business continuity by maintaining service delivery during adverse cyber events [13]. Consequently, analyses should focus on the business continuity, the minimum required vital services, and post-disturbance behavior of the system as a priority, rather than on IT systems or financial costs [14–18].

The resilience field traditionally emerged as a complementary component of risk assessment but gradually proliferated to the extent that resilience analysis is now an integral part of the risk field [19]. Cyber risk analysis on the other hand also plays a key role in fostering the resilience of a society [20]. Risk assessment is therefore a core part of both cybersecurity and resilience [21] as it enables embedding security controls, which is the main step towards the realization of secure-by-design and consequently ensures cyber resilience [22]. While risk assessment is essential to study uncertain threatening disruptions and to focus on the hazardous event, resilience ensures these systems can withstand and recover from disruptions, safeguarding the system's stability and focusing on the system's capability to face the disruptive events. Nevertheless, conventional risk assessment methods such as those outlined in ISO 31000 [23], COSO (Committee of Sponsoring Organizations) Enterprise Risk Management (ERM) [24,25], PMBOK (Project Management Body of Knowledge) [26], and other risk management standards and frameworks based on a probability-impact matrix (PIM) often fail to address the complexities and dynamic nature of modern digital and cyber–physical systems (CPSs) [27–30]. Specifically, a PIM evaluates risks based on their likelihood and potential impact, providing a snapshot of risk severity [23,31]. Yet, this method does not account for the nuanced interactions between different risk factors, nor does it consider the resilience of the system itself in adopting or recovering from these risks [32].

Cyber resilience engineering integrated with risk assessment offers a significant advancement in CI protection, covering both pre-disturbance and post-disturbance stages. The integration of these approaches focuses on how systems can adapt, recover, and continue to function effectively despite facing disruptions [7,33–37]. However, risk assessment methods, standards, and regulations for cyber resilience are overwhelming and in some cases overlapping. Selecting a minimum set of security requirements that properly address an organization's specific features while also complying with applicable standards and regulations has become increasingly challenging [38]. On the other hand, the body of knowledge of cyber resilience in many critical sectors is yet to develop. Alhidaifi et al. [9], in their review on cyber resilience, highlighted the necessity of a systematic literature review (SLR) of cyber resilience frameworks. In addition, Pavão et al. [39] identified only 14 relevant articles in their review of cyber resilience within healthcare information systems. This necessitates a comprehensive review of methods, standards, and regulations in this domain, which, to the best of our knowledge, has not yet been undertaken in the literature. To fill this gap, this paper conducts an SLR on methods, models, standards, guidelines, and legislative frameworks that enhance cyber resilience by integrating resilience engineering with risk assessment.

In particular, this study is designed to explore and answer key questions regarding methods, standards, and regulations that contribute to cyber resilience through risk assessment, making the following main contributions.

- Identifying and classifying different risk assessment methodologies used for cyber resilience;
- Pointing out and investigating key standards and guidelines used in studies related to cyber resilience;
- Providing an overview of relevant regulations influencing cyber risk assessment for cyber resilience;

- Highlights gaps in current research and practice, suggesting areas for further exploration in cyber resilience strategies.

By conducting an SLR on cyber risk assessment for cyber resilience, this study provides a cyber resilience perspective on cyber risk assessment methods, standards, and regulations. This in turn helps provide insight into the integration of cyber risk assessment and cyber resilience to realize a holistic cybersecurity approach considering pre- and post-incident protection. The study offers a structured overview of diverse risk assessment methodologies and frameworks used in different CI domains, related standards that provide requirements to support these methodologies, and legislation that regulates their implementation. In this way, cybersecurity managers, decision-makers, and practitioners may adopt a suitable set of cyber risk assessment tools for cyber resilience that are acknowledged by cybersecurity standards and comply with related regulations.

The remainder of this paper is structured as follows: Section 2 provides an overview of the relevant literature and foundational concepts. Details of the methodologies and techniques used in the research are set out in Section 3. The results of the SLR are presented in Section 4 and thoroughly discussed in Section 5. Finally, Section 6 concludes the paper, presenting research implications, limitations, and future scope.

2. General Background Review

2.1. Security Risk Assessment Standards

Risk assessment is a crucial step in the broader process of risk management, as it relies on a variety of internationally recognized standards that offer structured methodologies for managing and mitigating risks. These standards facilitate effective risk management processes; therefore, investigating risk assessment requires a thorough examination of the body of knowledge in risk management to identify all established standards. Additionally, standards provide industry-specific and general frameworks that guide organizations in aligning their risk management practices with best practices and regulatory requirements [21,38]. Table 1 presents a collection of widely recognized standards related to risk management.

Table 1. Key risk management-related standards.

Standard	Title	Description	Ref.
ISO 31000:2018	Risk Management Guidelines	Principles and guidelines for effective risk management across all industries.	[23]
ISO/TS 31050:2023	Guidelines for managing an emerging risk to enhance resilience	This document complements ISO 31000.	[40]
ISO 27005:2018	Information Security Risk Management	Guidelines for managing information security risks within organizations.	[41]
ISO/IEC 27001:2013	Information Security Management Systems (ISMSs)	Requirements for establishing and maintaining an information security management system with risk management processes.	[42]
ISO 22301:2019	Business Continuity Management Systems (BCMS)	Framework for identifying and managing risks that could disrupt business operations.	[43]
NIST SP 800-37	Risk Management Framework (RMF)	Guidelines for applying risk management to federal information systems in the United States.	[44]
COSO ERM Framework	Enterprise Risk Management	Integration of risk management into organizational strategy and performance.	[24,25]
IEC 31010:2019	Risk Management—Risk Assessment Techniques	Guidance on various risk assessment techniques.	[45]
ISO 22301, ISO 22313, ISO 22316	Organizational Resilience	Principles for enhancing organizational resilience through risk management.	[46]
ISO 14971:2019	Application of Risk Management to Medical Devices	Guidelines for applying risk management throughout the life cycle of medical devices.	[47]
ISO 37001:2016	Anti-bribery Management Systems	Techniques for robust internal controls and compliance processes that are crucial for addressing cyber threats exploiting corruption.	[48]

These standards provide frameworks and guidelines applicable across various industries and domains. For instance, ISO 31000:2018 [23] offers general principles and guidelines for risk management applicable to any organizational context. On the other hand, the ISO/IEC 27001 [49] focuses on information security risk management, particularly in protecting sensitive information within organizations.

2.2. Cyber Resilience

The term cyber resilience first appeared in published research in 2009 [50], making it relatively recent compared to related concepts like cybersecurity, which has been in use since 1980 [51]. Cyber resilience refers to the ability to prepare for, withstand, and recover from cyber disruptions while maintaining critical operations, particularly in those systems, organizations, missions, or business processes whose functioning and/or service delivery rely heavily on information technology (IT) systems [11,52]. Unlike cybersecurity and cyber defense, which focus on prevention, cyber resilience encompasses response, and recovery [53].

Critical components of cyber resilience include preparedness [54,55], adaptability [8,13,54–59], robustness [8,54,58,60], recovery [12,13,54,56–59], response [12,57], flexibility [8,56,59,60], and redundancy [8,12,55–58,58,59].

Most of the critical components of cyber resilience are interconnected and fundamentally rely on effective risk identification and assessment. Specifically, preparedness involves identifying potential threats and vulnerabilities to develop proactive measures and contingency plans [54,55]. Adaptability is the ability to modify and evolve strategies and systems in response to changing threat landscapes [8,13,54–59]. Robustness refers to the capacity to maintain core functions during a cyber incident, requiring a thorough understanding of risks to fortify CIs [8,54,58,60]. Recovery focuses on restoring operations quickly and effectively after a disruption, guided by pre-identified risks and vulnerabilities [12,13,54,56–59]. Response is the immediate reaction to a cyber incident, which must be planned based on anticipated risks [12,57]. Flexibility allows an organization to shift resources and strategies as threats evolve, informed by continuous risk assessments [8,56,59,60]. Finally, redundancy ensures that alternative resources and systems are in place to support critical functions in case of failures, necessitating prior identification of single points of failure and associated risks [8,12,55–59].

Exploring the recent literature and standards reveals that some methods and frameworks now integrate resilience and business continuity with traditional risk management practices. An example is the ISO 223XX series, which emphasizes continuity and resilience, aiming to prepare organizations for potential disruptions and enhance their ability to recover from unforeseen events [61–64]. Another example is PIMs, which are used widely to quantify the risk and strategic planning to increase adaptability [65], and efficiently address vulnerabilities [66,67]. Moreover, the COSO ERM Framework integrates risk management with strategic objectives [24], ensuring that risk is considered when making high-level decisions. Finally, specialized standards also address risk management in specific sectors, offering tailored guidelines, such as ISO 14971:2019 for medical devices [47].

2.3. Risk Assessment for Cyber Resilience

The integration of risk management approaches and cyber resilience is necessary to adequately address the protection of complex systems like CI [68]. Risk analysis (i.e., risk assessment and management) assumes that different kinds of 'known' uncertainties can raise identifiable hazards [69]. Resilience, on the other hand, intends to prepare for all kinds of uncertain hazardous events including 'unknown unknown' risks [70,71]. Risk analysis examines the system components to identify and characterize hazards while resilience analysis enhances the system's response to surprises. Therefore, although risk analysis and resilience are two different approaches to handling hazards, neither of them alone is sufficient to mitigate the impact of adverse disturbances [72]. Extending risk assessment to the cyber resilience approach is beneficial because it allows for considering the influence

of adverse events on the system's performance resilience curve [73]. The literature has addressed this integration in different ways, such as resilient cybersecurity risk assessment [74] and cyber-resilient risk assessment [68]. In this paper, this integration is referred to as risk assessment for cyber resilience. A 'resilience-aware' risk management produces 'resilience-related' controls that enhance the resilience capabilities of the system, i.e., to resist, absorb, adapt, and/or recover effectively and efficiently [68,75]. Risk assessment may play a key role here by analyzing the effectiveness of these controls and supporting decisions regarding the selection and prioritization of risk mitigation strategies to enhance CI resilience [75,76].

2.4. Literature Limitations and Research Gaps

Almost all conventional risk management frameworks and standards suggest the use of a PIM for risk assessment [77] because of its simplicity and effectiveness in a long-shot perspective of a complex system, and in qualitatively prioritizing risks [78]. However, it has notable drawbacks, as follows:

1. Subjectivity and bias: The PIM relies on expert judgment to estimate the probability and impact of risks [79]. Different stakeholders may have varying perceptions, leading to inconsistencies and biases in the scoring. This reliance on subjective opinions can undermine the matrix's effectiveness [79,80].
2. Limited criteria consideration: Typically, there is a need for requirement analysis to select the right criteria in multi-criteria problems [81–83]. PIM considers only two factors: probability and impact. Real-world risks are often more complex and influenced by additional criteria such as time sensitivity, interdependencies, and resource availability [84,85]. This oversimplification can lead to inaccurate prioritization.
3. Lack of precision: Although accuracy is a hot topic in uncertainty analysis [86–89], PIM usually categorizes risks into broad, qualitative ranges (e.g., low, medium, high) rather than using precise quantitative values [90]. This lack of granularity can cause ambiguity, especially when risks fall near the boundaries of these categories, hindering effective decision making.

On the other hand, the way that PIM is used raises some challenges and faces some limitations, as follows:

1. Limitation in inability to handle interdependencies: Risks are often interconnected, with one risk potentially triggering or amplifying another. On the other hand, the emerging systems and infrastructures are also interconnected. The PIM does not adequately account for these interdependencies, leading to an incomplete understanding of the overall risk landscape [91].
2. Static nature challenge: PIM is typically used as a one-time assessment tool. However, risks evolve over time [92,93], and their probability and impact can change. The static nature of PIM limits its ability to dynamically adjust to these changes. Updating the PIM periodically introduces several challenges. First, frequent updates require additional resources, including time, personnel, and funding, which can strain organizational capacity. Second, collecting accurate and up-to-date data to reassess risks can be complex, particularly if external conditions or internal structures change rapidly. Additionally, periodic updates may lead to inconsistencies in results if the assessment criteria or methodologies are not standardized over time. Finally, scheduling regular updates while maintaining accuracy and relevance adds logistical complexity, requiring careful planning to avoid disruptions to regular operations.

Additionally, the wide range of risk assessment methods, standards, and regulations related to cyber resilience creates confusion due to overlapping frameworks, making it challenging for organizations to select appropriate security requirements that meet their needs and compliance obligations. Nevertheless, there is a significant gap in the literature to systematically examine the empirical use of risk assessment methods, standards, guidelines, and globally known legislation to enhance cyber resilience. This paper addresses the lack

of a comprehensive review in this area by conducting an SLR on approaches that integrate cyber resilience engineering with risk assessment.

3. Materials and Methods

3.1. Research Design

This paper adopts an SLR approach to explore research on risk assessment for cyber resilience. It is structured in accordance with the guidelines for SLRs in the management field [94]. Specifically, the SLR process consists of three key phases: planning the review, conducting the review, and reporting and dissemination. In the planning phase, the necessity of an SLR on risk assessment for cyber resilience is established, while the conducting phase involves a systematic search, filtering, and analysis of relevant studies using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines [95]. Finally, the reporting phase organizes the review findings to draw valuable insights. The study adheres to the PRISMA method to ensure transparency and reproducibility, shown in Figure 1.

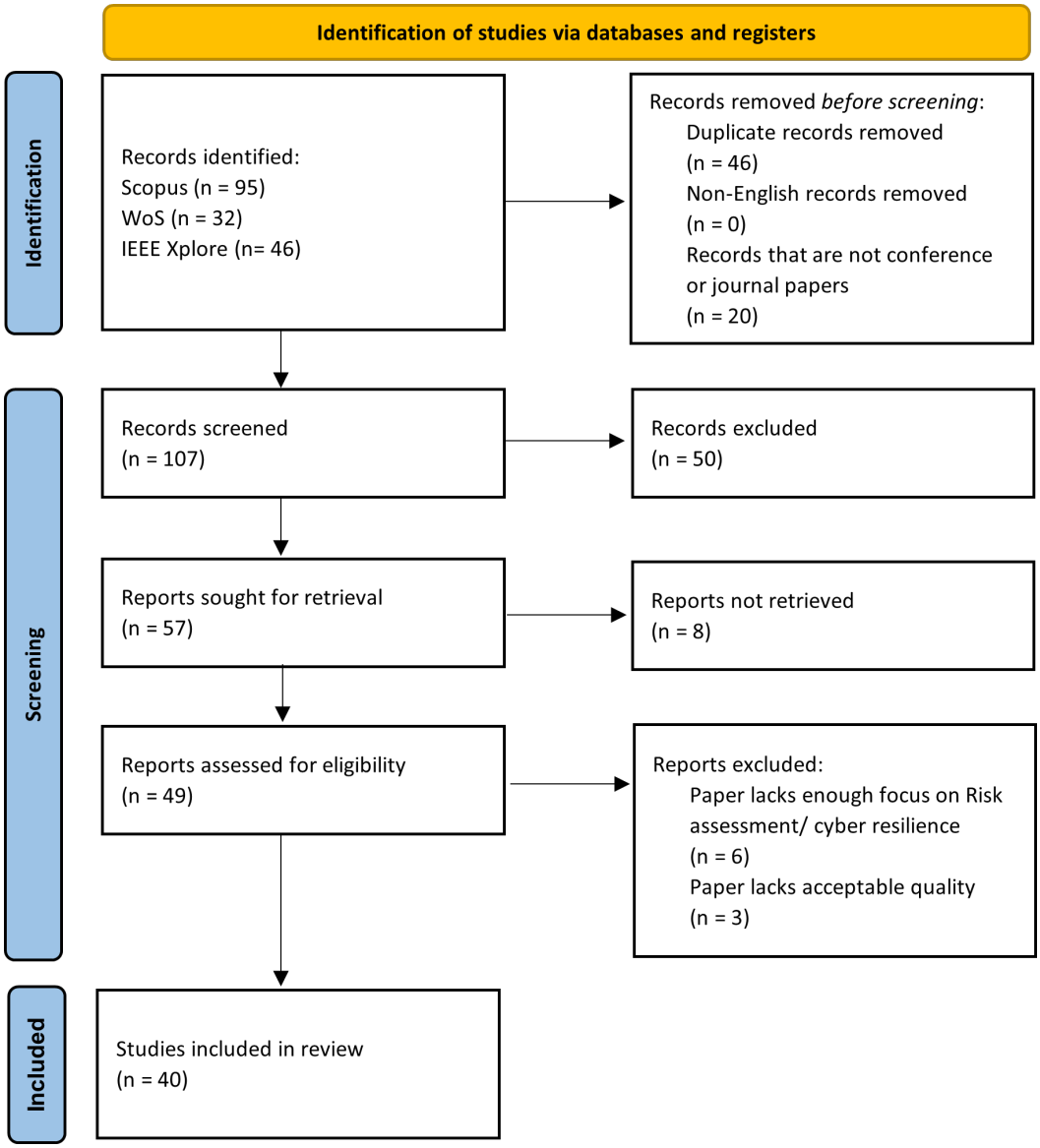

Figure 1. Research design flowchart.

3.2. Data Attributes

In addition to addressing specific research questions (detailed in next section), this review first takes a broader approach by providing bibliometric and scoping insights to contextualize the literature landscape. Key data attributes were collected from each selected paper; these were as follows:

- Number of yearly publications by source type: Tracks the volume and source types (e.g., journals, conferences) of publications over time, reflecting trends and shifts in scholarly attention toward resilience enhancement in risk assessment.
- CI sectors addressed: Identifies the focus sectors (e.g., energy, transportation) targeted by each paper, providing insight into which CI areas are prioritized in resilience-related studies.
- Author keywords: Lists the most frequently occurring keywords, indicating prominent themes within the literature.
- Inter-article connectivity via shared topics: Examines the network of articles interconnected by shared topics, highlighting collaborative patterns and thematic linkages across studies.

These attributes offer a comprehensive overview of the research landscape, helping to identify significant patterns, emerging topics, and potential gaps in the resilience-related risk assessment literature (reported in Section 4.1), which provides foundational knowledge before a full paper analysis aimed at answering the research questions derived from the literature.

3.3. Research Questions

The SLR in this paper aims to answer three key research questions (RQs) related to cyber resilience through risk assessment. To ensure a consistent comparison of information across the analyzed studies, we followed a similar methodology as used by Lezzi et al. [96], where each RQ is linked to a specific area of analysis. Table 2 outlines the three RQs along with their corresponding areas of analysis, providing a clear structure for addressing the focus of this research. As seen in the table, the research questions are designed in a way that each addresses a main element of the SLR. The focus of RQ1 is on papers that conduct risk assessment methodologies considering cyber resilience in their study. The intention of designing RQ2 is to investigate related normative documents (e.g., standards, guidelines, frameworks) mentioned by these studies. Finally, RQ3 intends to provide insight into how related regulations and legislative documents support the implementation of these methods.

Table 2. Research questions and areas of analysis for cyber resilience study.

No.	Research Question	Area of Analysis
RQ1	What are the methodologies used to address cyber resilience through risk assessment?	Identifying risk assessment methodologies that take cyber resilience into account.
RQ2	Which standards are considered by studies that focus on risk assessment for cyber resilience?	Exploring the standards, frameworks, guidelines, etc., frequently cited in risk assessment studies that consider cyber resilience.
RQ3	What regulations are relevant to risk assessment for cyber resilience?	Investigating relevant regulations; examining how legal frameworks impact risk assessment practices for cyber resilience.

3.4. Search Process

The search string used in this study incorporates three sets of keywords. The selection of keywords for this study was carefully carried out following the established guidelines for conducting SLRs in the resilience field, as outlined by Ardebili and Padoano [32]. This approach ensures a comprehensive and structured process for identifying relevant literature, allowing the study to capture a wide range of sources while maintaining focus on the key themes of interest. Table 3 summarizes the results of the research queries applied

to Scopus, Web of Science (WoS), and IEEE Xplore (see Table 3); these were used as they are widely regarded as some of the most comprehensive and inclusive academic databases in the fields of computer science and more specifically cybersecurity and resilience [97,98].

Table 3. Search queries and results. QTY: Number of document results. Asterisk (*) at the end of a word indicates that all variants of the word are also included.

Query ID	Search in	Query String	QTY
Qs[#doc.]	Scopus	TITLE-ABS-KEY (“cyber resilien*” AND “risk assessment”)	95
Qw[#doc.]	WoS	TS = (“cyber resilien*” AND “Risk assessment”)	32
Qi[#doc.]	IEEE	“cyber resilien*” AND “risk assessment”	46

The queries used in the different databases include searching in titles, abstracts, and keywords to find articles containing keywords “cyber resilience” and “risk assessment”. These search strings retrieve any document that explores both cyber resilience and risk assessment, irrespective of the scope of the study, type of document, or application domain. This approach ensures that the results are comprehensive and inclusive, covering a wide spectrum of studies relevant to our research.

3.5. Analysis Criteria

Table 4 outlines the criteria used for screening records in the SLR. The exclusion criteria include records not written in English, non-peer-reviewed publications like editorials or book chapters, and studies unrelated to cyber resilience or risk assessment. Conversely, the inclusion criteria ensure that only studies are selected that provide insight into cyber risk assessment for cyber resilience or discuss related standards, guidelines, or regulations. Applying these criteria helps refine the selection to ensure that the most pertinent papers are included for a comprehensive analysis addressing the research questions. In the following sections, the results are reported and discussed in depth.

Table 4. Exclusion and inclusion criteria for record screening.

Criteria Type	Criterion
Exclusion Criteria	1. Records that are not written in English. 2. Records that are published as technical opinions, editorials, testimonials, organizational reports, book series, or book chapters. 3. Studies that do not discuss cyber risk assessment or cyber resilience.
Inclusion Criteria	1. Studies that propose, perform, or validate the cyber risk assessment methods with a cyber resilience perspective 2. Studies that discuss standards, guidelines, or regulations related to risk assessment for cyber resilience.

4. Results

The current section is dedicated to providing an overview of the SLR’s findings according to three main areas of analysis: risk assessment-related methods and models, risk assessment-related standards, and risk assessment-related governance. This summary aims to highlight key methodologies utilized in risk assessment, outline relevant standards and frameworks that guide risk management practices, and itemize pertinent regulatory and legislative frameworks that shape compliance and governance in risk management processes.

4.1. General Synthesis of Results

Before presenting the results of the SLR, a general synthesis of the reviewed papers is provided in this subsection to provide a ‘bird’s-eye view’ of the investigated knowledge area. As shown in Figure 1, 40 papers were included in the review, which together constitute

the knowledge area of 'risk assessment for cyber resilience'. These papers are analyzed according to their publication year, source type, sectors addressed, and keyword analysis.

Figure 2 illustrates the annual number of publications, divided by their source type. The first publication was a conference paper [22], published in 2016, followed by only one conference paper in the entire 2017. The first journal paper was published the next year, in the IEEE Systems Journal [99]. Moreover, the cumulative percentage curve indicates that more than half of all documents considered in the review were published in 2023 and 2024. This suggests the potential for significant growth in the next few years. Moreover, half of the publications are journal articles while the other half are conference papers.

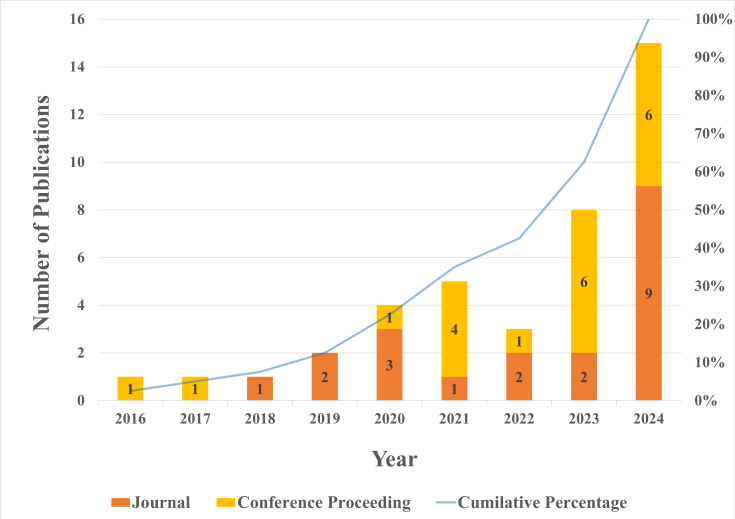

Figure 2. Number of yearly publications categorized by source type.

While reviewing the papers, we realized that some of them specifically address a certain CI sector. Therefore, in Table 5 we grouped the papers by the CI sector they focus on. The categories are extracted from the 16 CI sectors introduced by the Cybersecurity and Infrastructure Security Agency (CISA) of the United States [100]. As shown in the table, nine papers focused on the transportation system CI sector. More specifically, papers in this sector focused on the automotive [68,101,102], aviation [22,103–105], and maritime [106,107] domains. In the energy sector, eight papers were found, all of which addressed the smart grid domain. In the healthcare and public health sector, papers focused on Medical CPS [108], healthcare information systems [109], and healthcare cyber systems [110]. Finally, papers in the IT sector investigated artificial intelligence (AI) [111,112] and cloud services [113].

Table 5. CI sectors addressed by the considered papers.

CI Sector	Ref.
Transportation systems sector	[22,68,101–107]
Energy sector	[114–120]
Healthcare and public health sector	[108–110]
IT sector	[111–113]
Emergency services sector	[121]
Communication sector	[99]
Not categorized	[9,20,39,122–134]

The keyword analysis results in Figure 3 show the most frequently occurring keywords across the articles reviewed. Specifically, Figure 3 highlights a strong emphasis on

cybersecurity and threat analysis and modeling in the literature. Additionally, the network visualization in Figure 4 represents the relationship between articles and shared keywords. Each article is connected to the keywords it uses, showing how different articles overlap based on common topics. The most central keywords in this network are National Institute Standards and Technology (NIST), framework, goals, and anticipation. This figure shows that articles related to "cyber resilience" and "NIST" are likely discussing frameworks or standards for assessing and improving resilience in cybersecurity.

In Figure 4, the concepts of physical security, cybersecurity, risk, and IoT are all interlinked through the paper Qi4 [128]. As interpreted from the figure, IoT acts as a key enabler in merging physical infrastructure with digital systems, hence opening the door for real-time data collection, analytics, and reactive measures in risk assessment frameworks. The interplay between these components highlights the increasing importance of IoT as a key point to be considered for integrated risk management in cyber–physical systems (CPSs) [135]. This implies that future studies could focus on understanding and extending the role of IoT in the risk management related to CPSs, specifically in addressing cyber–physical vulnerabilities.

However, a limitation can be noticed in Figure 4. The model depicted in the figure shows a lack of social aspect considerations. As per the new complex system definition [136], the social part includes human behaviors, organizational dynamics, and societal impacts. Cyber–physical social systems (CPSSs) include social aspects interacting with cyber and physical elements, thus creating interdependencies and potentially introducing new types of risks. Although digital technologies, such as digital twin, have been proposed as solutions to enhance resilience in CPSSs [30], the vulnerabilities and corresponding solutions of CPSSs are not widely studied.

A separate network of frequently used keywords is shown in Figure 4; it revolves around the paper Qi1 [129]. It involves resilience features such as recovery, resistance, anticipation, and adaptation. These features are interlinked within the same network, alongside the 'NIST' standard, illustrating the importance of aligning resilience attributes with established regulatory frameworks and best practices.

Finally, as shown in Figure 4, cutting-edge technologies such as digital twin and blockchain are in the same network as the keywords "critical performance indicators" and "critical success factors", where the study Qs59 [117] is located. This relationship further signifies the need to create quantitative metrics for resilience attributes.

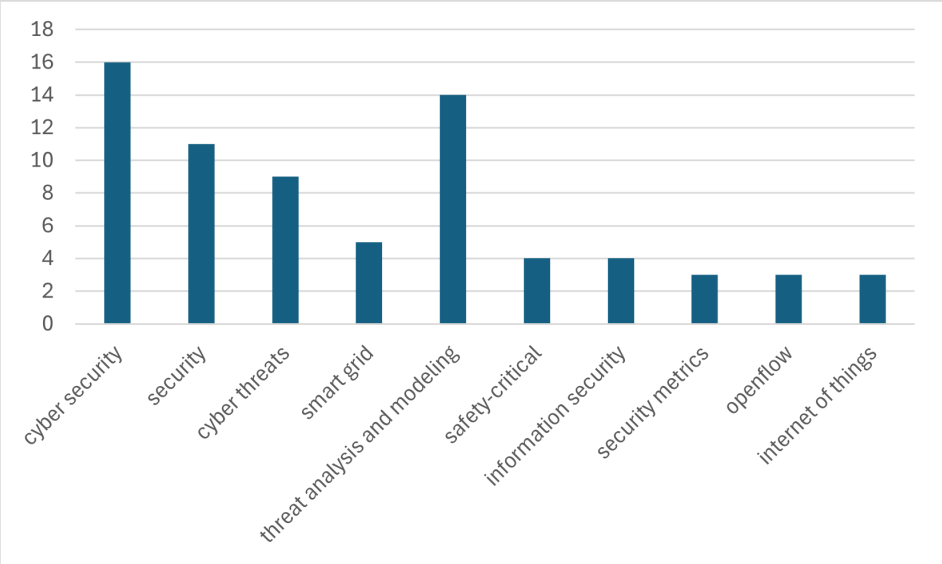

Figure 3. Most frequently occurring keywords across the articles reviewed. The keywords that are used in the search query like resilience and cyber are not considered.

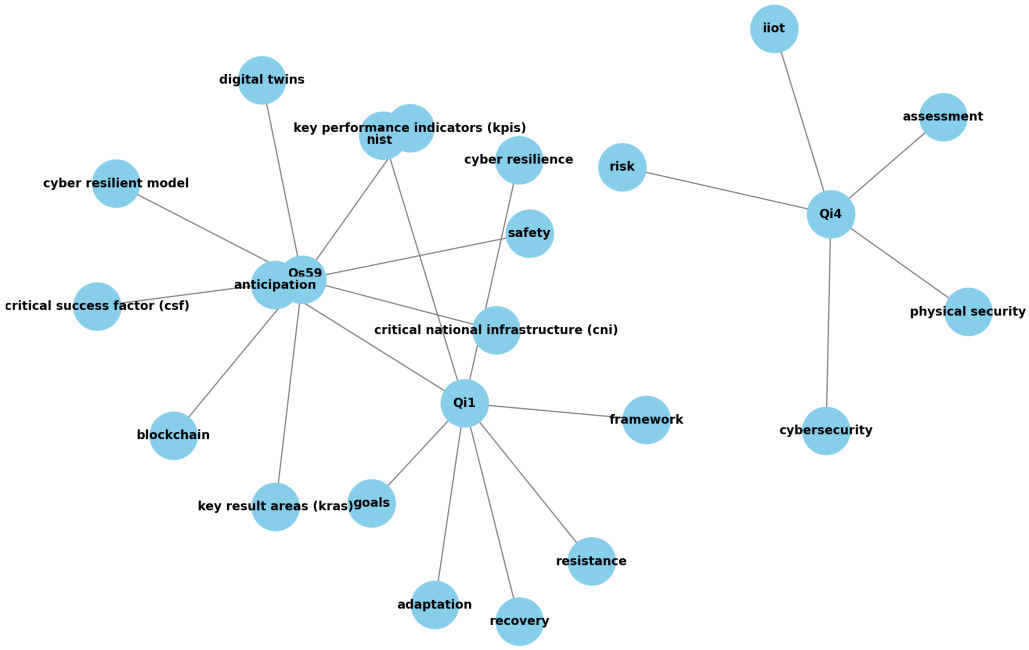

Figure 4. The network of the interconnectivity of articles through shared topics. An ID is assigned to the articles to increase the readability of the graph that is available in Appendix A.

4.2. Risk Assessment-Related Methods and Models

The SLR unveiled risk assessment-related methods and models that offer structured approaches to evaluate and mitigate cyber threats, leading to enhanced cyber resilience. Methods like qualitative and quantitative risk assessments help prioritize risks, while models such as Bayesian networks and attack graphs provide insights into threat scenarios and mitigation strategies [137,138]. The current challenge is to understand how various techniques are applied in practice, identify their effectiveness, and develop more robust cyber resilience strategies tailored to specific domain needs [139]. The identified risk assessment methods and models are reported in Table 6, providing for each the title, a brief description, and the category to which it belongs.

Table 6. Risk assessment/management-related methods, tools, methodological frameworks (M.F.s) and models.

Ref.	Title	Description	Cat.
[22]	Probability-Impact Matrix	Method that uses probability and impact to assess risks within the STRIDE categories.	Method
[116]	Risk Quantification (TVI)	Risk assessment method calculating risk based on threat, vulnerability, and impact factors. Risk = Threat × Vulnerability × Impact.	Method
[111,140]	AI-Enabled Risk Assessment	Risk identification, probability, and impact assessment supported by AI models like ChatGPT.	Method
[22]	SecRAM by SESAR SWP16.2	Security risk assessment methodology specific to SESAR projects. Tailored to network systems using probability-impact assessments, focusing on confidentiality, integrity, and availability (CIA) of primary assets.	Method
[116]	CCE Scoring Method	Method used for assessing impact in risk management.	Method
[117]	Risk Assessment: ICS Cyber Killchain	Methodology for assessing impact through cyber kill chain analysis.	Method
[117]	Cybersecurity Capability Maturity Model (C2M2)	Maturity model for evaluating and improving cybersecurity capabilities.	Model

Table 6. *Cont.*

Ref.	Title	Description	Cat.
[109]	Endsley's Three-Level Model of Situational Awareness	Model for understanding and developing situational awareness.	Model
[130]	OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation.	Method
[130]	FAIR	Factor Analysis of Information Risk.	Method
[130]	CRAMM	Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Method.	Method
[117]	CVSS	Common vulnerability scoring system (CVSS); for measuring the severity of vulnerabilities.	Method
[101]	STRIDE Threat Model	Threat modeling method focusing on six categories: Spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.	Model
[9]	PASTA	Threat modeling method used to align technical requirements with business objectives.	Model
[9]	DREAD	Method for risk assessment that evaluates threats based on five factors: Damage, reproducibility, exploitability, affected users, and discoverability (DREAD).	Method
[121]	Holistic Risk Assessments	Assessment method considering interconnected and interdependent risks, such as disaster risks, cybersecurity risks, and cascading effects.	Method
[114]	Security Score Model	Model that quantifies security based on predefined scoring criteria.	Model
[130]	Direct Testing Method	Risk assessment through audit, exercise, and penetration testing.	Method
[115]	Five-Phase Resilience Assessment Framework	Framework based on Bayesian network that quantifies resilience contributors in five phases.	M.F.
[110]	RAMA	Framework for risk analysis using factors like probability, impact, historical data, and contextual relevance.	M.F.
[105]	ICAO Security Risk Assessment	Methodology for security risk assessment using probability and impact in aviation security.	Method
[101]	TARA (Threat Analysis and Risk Assessment)	Combination of STRIDE for categorizing threat scenarios and DREAD for quantifying feasibility, likelihood, and impact.	Method
[101]	System Security Risk Assessment (SSRA)	Method defined by DO-326A/ED202A for security risk assessment in systems.	Method
[131]	Logical Attack Graph (LAG)	A method for visualizing potential attack paths and assessing their impact on systems.	Method
[131]	Mission Impact Propagation Graph (MIPG)	Graph-based method for assessing how cyber-attacks propagate through missions.	Method
[131]	Mission Impact Assessment Graph (MIAG)	Graph-based method for assessing the impact of threats on mission-critical operations.	Method
[39]	Event Tree Analysis	Systematic approach for analyzing the possible outcomes following an initial event.	Method
[39]	Physical and Cyber Risk Analysis Tool (PACRAT)	Tool for conducting comprehensive risk analysis that includes both physical and cyber threats.	Tool
[117]	Threat, Vulnerability, and Risk Analysis (TVRA)	Method for assessing threats, vulnerabilities, and overall risk in systems.	Method
[117]	i-TRACE Risk Assessment	Framework for risk assessment combining traceability and vulnerability management.	M.F.
[107]	SOHRA (Shipboard Operation Human Reliability Analysis)	Method for assessing human error probability in shipboard operations.	Method
[20]	Extreme Value Theory (EVT)	Statistical approach for modeling extreme risk events in cybersecurity.	Model

Table 6. *Cont.*

Ref.	Title	Description	Cat.
[20]	Stochastic Hybrid Model	Hybrid approach combining stochastic methods with traditional risk assessment models.	Model
[20]	Tail Threshold Detection	Method for identifying the threshold above which risk events are considered extreme.	Method
[114]	SDN-Based Mitigation	Mitigation of risks using software-defined networking principles.	Method
[134]	IED Criticality Assessment	Assessment of the criticality of intelligent electronic devices in industrial systems.	Method
[114]	Cyber Attack Modeling	Modeling and assessing the impact of denial of service attacks.	Method
[22]	Probability-Impact through the SecRAM	Risk assessment methodology focusing on probability and impact, tailored for network systems.	Method
[108]	Vulnerability-Impact-Likelihood	A formulaic approach to quantifying risk based on vulnerability, impact, and likelihood.	Method
[132]	Raising Awareness	Promoting cybersecurity awareness among IT/OT end users.	Activity
[104]	Human Error Probability Assessment	Assessing the probability of human error in system operations.	Method
[109]	Fault Tree Analysis	Method for analyzing system failures and identifying potential causes.	Method
[129]	Risk Management Strategy (RMS)	Strategic approach to managing and mitigating risks in organizations.	Strategy
[128]	Taxonomy-Driven Risk Assessment	Risk assessment methodology using a structured taxonomy to categorize and evaluate risks.	Method
[133]	Threat Intelligence (TI) Module	Component for collecting and analyzing threat data to improve risk assessments.	Tool

Lastly, some documents not specified in the table—such as Bank for International Settlements (BIS) [141]—recommend other standards, methods, and guidelines to increase resilience, but do not specify any particular risk assessment methods themselves. Furthermore, some documents such as the Digital Operational Resilience Act (DORA) [142], and the World Economic Forum's (WEF's) [143] "The Cyber Resilience Index: Advancing Organizational Cyber Resilience", only recommend regular risk assessment as a key practice to enhance cyber resilience [144]. However, these documents do not prescribe specific risk assessment methods; rather, they provide general recommendations, encouraging organizations to perform assessments consistently.

4.3. Risk Assessment-Related Standards

The SLR revealed that studies on cyber resilience should consider risk assessment-related standards, guidelines, and frameworks because they provide structured methodologies for identifying, evaluating, and mitigating cyber risks in a consistent and effective manner. Specifically, standards (such as ISO/IEC 27001) offer a comprehensive approach to information security management, while frameworks (like the NIST Cybersecurity Framework) provide a set of best practices for improving cyber resilience across various industries. Moreover, guidelines (from bodies like ENISA and the European Commission) ensure that these frameworks are aligned with regulatory requirements and industry-specific challenges. The results of this section are listed and defined in Table 7, which provides essential background to understanding the diverse methodologies used in the literature for assessing and enhancing cyber resilience.

Table 7. Risk assessment-related standards (Stds.), guidelines (Gdls.), and frameworks (Fwks.).

Ref.	Name	Description	Cat.
[102]	ISO 21434: Automotive Cyber Security	Standard focusing on cybersecurity for road vehicles.	Std.
[116]	Risk Management Architecture: INL Framework	Aligning with the NIST framework for managing cybersecurity risks.	Fwk.
[116]	IEEE 1547.3	Guide for cybersecurity of distributed energy resources interconnected with electric power systems.	Std.
[107,120,122,133]	ISO/IEC 27001	Information security management standard.	Std.
[107,109,113,120,122,124,127,133,134]	NIST Cybersecurity Framework (CSF)	Guidelines for improving CI.	Gdl.
[9]	Cyber Resilience Framework (CRF)	Structured approach for ensuring resilience in information systems.	Fwk.
[9]	CERT Resilience Management Model (CERTRMM)	Framework for managing operational resilience.	Fwk.
[9,112]	COBIT	Framework for enterprise IT governance and management.	Fwk.
[9,128]	OWASP	Open Web Application Security Project framework for software security.	Fwk.
[121]	Sendai Framework for Disaster Risk Reduction 2015–2030	Global strategy for reducing disaster risk and building resilience.	Fwk.
[121]	UN Guidelines on Man-Made and Technological Hazards	Guidelines provided by the UN Office for Disaster Risk Reduction (DRR).	Gdl.
[130]	ISO 27001:2013	Updated version of ISO 27001 focusing on information security management.	Std.
[109,120,122,130,133]	ISO 27005	Risk management standard for information security.	Std.
[22]	ISO 31010	Standard for risk assessment techniques.	Std.
[117,132]	ISO 31000	Guidelines for risk management.	Std.
[22,68,108,118,123,144]	NIST SP 800-30	Guide for conducting risk assessments.	Gdl.
[22,129,144]	MITRE	Framework for threat analysis and mitigation.	Fwk.
[22,133]	ENISA	European Union Agency for cybersecurity recommendations and guidelines.	Gdl.
[112]	COBIT 2019	Updated COBIT framework for IT governance and management.	Fwk.
[112]	ISO 42001:2023	Standard for governance, risk, and compliance (GRC).	Std.
[115]	NISTIR: Guidelines for Smart Grid Cybersecurity	Guidelines for cybersecurity of smart grids.	Gdl.
[111]	NIST AI RMF	NIST AI risk management framework for managing AI risks.	Fwk.
[22]	DO326A/ED-202A	Guidelines for cybersecurity in aviation.	Gdl.
[129]	NIST SP 800-160, Volume 2	Systems security engineering guidelines.	Gdl.
[134]	IEC 61850	International standard for communication networks and systems in substations.	Std.
[39]	ISO/SAE 21434:2021	Standard for cybersecurity engineering in road vehicles.	Std.

Table 7. *Cont.*

Ref.	Name	Description	Cat.
[117,119]	NERC-CIP	North American Electric Reliability Corporation CI Protection standards for securing bulk power systems.	Std.
[106]	IMO MSC.428 (Maritime Cyber Risk Management)	Guidelines for integrating cyber risk management into the safety management systems (SMSs) of vessels.	Gdl.
[106]	IACS E26 and E27	Cybersecurity guidelines for new vessels, issued by the International Association of Classification Societies.	Gdl.
[106]	BIMCO Cyber Security Guidelines	Guidelines provided by the Baltic and International Maritime Council for managing cybersecurity on ships.	Gdl.
[106]	Safety4Sea STCW Convention Guidelines	General guidelines for officers under the STCW Convention, with a focus on cybersecurity.	Gdl.
[119]	Cybersecurity and Infrastructure Security Agency (CISA) Report	Report by CISA providing insights into cybersecurity threats and defense strategies.	Rpt.
[110]	ENISA Cybersecurity Skills Report	Report by the European Union Agency for Cybersecurity on developing cybersecurity skills in the EU.	Rpt.
[127]	Cyberthreat Defense Report (CDR)	Annual report highlighting trends and data on cyber threats and defenses.	Rpt.

4.4. Risk Assessment-Related Governance and Lawmaking

This study considers all elements in the context of lawmaking and governance including regulations, legislation, and directives, because each plays a crucial role in shaping the legal and operational landscape of cyber resilience. Specifically, legislation provides the foundational legal framework that establishes broad principles and mandates for cybersecurity across jurisdictions. On the other hand, regulations offer specific, enforceable rules derived from this legislation, ensuring compliance and setting detailed standards for cyber defense mechanisms. For instance, the General Data Protection Regulation (GDPR) in the EU directly influences how organizations manage data security and respond to breaches. Finally, directives, particularly in the European context, set goals for member states to achieve in areas like CI protection, allowing each country to implement the necessary measures through national laws.

The legal obligations, compliance requirements, and strategic frameworks that influence the development and implementation of cyber resilience strategies are extracted from the literature and studied in depth to answer the related research question. Table 8 details the identified regulations, directives, legislation, and acts.

Table 8. Risk assessment-related regulations (Regs.), directive (Dirs.), regulatory framework (RegFs), acts (Acts) and others (Oths.). The column Cat. shows the category of the row.

Ref.	Name	Description	Cat.
[104,109,117, 128,132,133]	NIS Directive	Directive focusing on the security of network and information systems in the EU.	Dir.
[132]	EU Proposal for NIS 2.0	Proposal for an updated Network and Information Systems Directive.	Dir.
[104]	European Community EC/216/2008 Regulation	Regulation concerning data security and protection in the European Community.	Reg.

Table 8. *Cont.*

Ref.	Name	Description	Cat.
[107]	Maritime Safety Management System (SMS) Requirements	Requirements for integrating cyber risk management into maritime SMS.	Oth.
[106]	STCW Convention	International convention outlining general requirements for seafarers, including cybersecurity.	Oth.
[109]	HIPAA	Health Insurance Portability and Accountability Act governing data security and privacy in the US healthcare sector.	Act
[121]	EU Cybersecurity Act (CSA)	Regulation to strengthen the security of network and information systems across the EU.	Reg.; Act.
[102]	UNECE Regulation	United Nations Economic Commission for Europe regulations focusing on vehicle safety and cybersecurity.	Reg.
[121]	National Risk Register, UK (2016)	Report outlining the key risks faced by the United Kingdom, including cybersecurity threats.	Oth.
[121]	National Risk Analysis, Norway (2014)	Analysis detailing the primary risks facing Norway, with emphasis on national security.	Oth.
[121]	Security Strategy for Society, Finland Security Committee	Strategy document that outlines Finland's approach to security, including cyber resilience.	Oth.
[121]	National Safety and Security Strategy, The Netherlands	Strategy for enhancing safety and security in the Netherlands, addressing cyber risks.	Oth.
[99]	European Operational Concept Validation Methodology (EOCVM)	Methodology for validating operational concepts within the EU.	Oth.
[112]	EU AI Act	Regulation proposed by the European Union to govern artificial intelligence and its use.	Reg.
[105]	International Civil Aviation Organization (ICAO) Aviation Cybersecurity Strategy	Strategy for managing cybersecurity risks in international civil aviation.	Oth.
[101,103]	European Union Aviation Safety Agency (EASA) Concept Paper	Concept paper outlining the approach to aviation safety, including cybersecurity.	Oth.
[131]	US Department of Energy Cybersecurity Frameworks	Frameworks and guidelines for ensuring cybersecurity in the energy sector.	RegF
[39,68]	UN Regulation No. 155 on Cybersecurity	Regulation focusing on cybersecurity management systems for vehicles.	Reg.
[132]	Presidential Policy Directive 21 (PPD-21/2013)	US directive focusing on the security and resilience of CI.	Dir.
[132]	Cybersecurity Enhancement Act of 2014	US law to promote cybersecurity research, development, and public–private partnerships.	Act
[132]	Executive Order (EO) 13636	US executive order aimed at improving CI cybersecurity.	Act
[109,117,132]	EU Regulation 2016/679 (GDPR)	General Data Protection Regulation governing data protection and privacy in the EU.	Reg.
[132]	National Framework for Cybersecurity and Data Protection (FNCS&DP)	Framework for ensuring cybersecurity and data protection at the national level.	RegF.
[127]	Saudi Arabian Monetary Authority (SAMA) Cybersecurity Framework	Cybersecurity framework used in Saudi Arabia for financial institutions.	RegF.

5. Discussion

In this study, an SLR was conducted on academic papers that explored methodologies, standards, and regulations for risk assessment with a cyber resilience perspective. For this purpose, the review centers on three research questions, elaborated in Table 2. Using

the results of the SLR, presented in Section 4, the answers to the research questions are provided in this section.

5.1. Risk Assessment Methods for Cyber Resilience

Risk assessment with a perspective of cyber resilience is manifested by a 'security-by-design' mindset, enabled by continuous risk assessment and risk mitigation through suitable security measures [105]. Therefore, continuous monitoring is what connects risk assessment with cyber resilience [110,123]. In other words, to build and sustain cyber resilience, cybersecurity measures need to be continuously assessed and examined [119].

Researchers have used a variety of risk assessment methodologies to address cyber resilience, with noticeable differences and similarities. The difference between some methodologies emerges from different views on the elements that constitute risk. Huda et al. [108] considered risk as vulnerability, impact, and likelihood. Their risk assessment approach included asset identification through the Cyber Resilience Review (CRR) framework, threat source identification, vulnerability identification, attack model generation, impact estimation, and risk calculation. Conversely, Culler et al. [116] and Khanna and Govindarasu [119] viewed risk as the threat, vulnerability, and impact. Culler et al. [116] quantified threat impacts using the Cyber-informed Engineering (CCE) scoring method. Khanna and Govindarasu [119], on the other hand, calculated the impact by estimating the drop in resiliency before and after the occurrence of the threat event. They used the C2M2 model and suggested translating the vulnerabilities into vulnerability scores using the common vulnerability scoring system (CVSS) score [117]. For vulnerability, Culler et al. [116] utilized the common attack vectors that exist in different systems' layers.

Other types of risk assessment methods are based on the PIM approach, which consists of a threat analysis followed by a risk analysis method, often referred to as TARA. For threat analysis, studies mostly benefited from the STRIDE framework [9]. Examples of this are the System Security Risk Assessment (SSRA) [103], the TARA performed by Siddiqui et al. [101], Threat, Vulnerability, Risk Analysis (TVRA) [110,117], and the probability-impact risk assessment presented by Strandberg et al. [102]. For risk analysis, the most used framework is DREAD [9,101,103]. Moreover, some papers proposed their own factors for determining the probability and impact of threats. For probability, Elmarady and Rahouma [105] proposed factors such as required knowledge or expertise, historical data of occurrence of such threats, and cost and accessibility of the tools used to conduct the attack. For the impact, they considered the worst-case scenario of each threat, considering impacts on safety, efficiency/effectiveness, and financial, political, and reputational consequences. Asgari et al. [99] introduced a tailored Security Risk Assessment SecRAM, previously adopted in another study Asgari et al. [22], which also utilizes the probability-impact approach. For impact, they identified a set of primary assets. Then, they considered several critical impact areas, categorized as personnel, capacity, performance, economic, branding, regulatory, and environment. Then, they evaluated the impact based on the compromise of confidentiality (C), integrity (I), and availability (A). The probability, on the other hand, was divided into exposure to the threat source, and the potentiality that the threat source would occur.

Another approach to incorporating cyber resilience in risk assessment observed in the literature is to consider the probability and impact of threats and add other cyber resilience factors to the risk elements. Smyrlis et al. [110] presented the Risk Assessment and Medical Applications (RAMA), in which the risk analysis factors are probability, impact, historical data, and contextual relevance. They proposed RAMA as a multi-layer solution to evaluate the attack surface and resilience. Park and Park [68] presented a TARA methodology, called Probability, Impact, Exposure, and Recovery, with the aim of enhancing cyber resilience through risk assessment. In the method they presented, the probability is determined using the likelihood of attack based on skills, preparation time, and defense system; the impact is calculated considering the potential damage to safety-critical systems; exposure is defined

as the vulnerability of the system to being attacked; and recovery is measured through the system's ability to recover from an attack.

The classification of risk assessment and management techniques for improving cyber resilience, as shown in Table 9, demonstrates a number of strategies tailored to fit specific organizational needs that range from relatively simple quantitative methods to quantitative scoring systems and specialized models. Each of the categories—quantitative, qualitative, hybrid, and specialized—has unique methodologies, applications, and competencies required.

Quantitative methods are based on measurable parameters; they provide numerical risk estimations using various scoring criteria, such as probability, vulnerability, impact, and risk thresholds. For example, the PIM methodology, as cited in [22], uses a matrix format for assessing risks related to STRIDE classifications. Similarly, CVSS [117] is a standardized measure that allows for calculating the severity of vulnerabilities, and therefore quantifying and prioritizing security weaknesses. DREAD [9] estimates threats through multidimensional assessment to provide a holistic view of potential consequences. More sophisticated techniques, such as the CCE scoring method [116] and Tail Threshold Detection [20], offer greater precision by considering risk impact assessments and identifying thresholds for extreme events, respectively. Application of such quantitative approaches requires a certain level of statistical analysis skills and the ability to properly apply and interpret scoring models, which makes them particularly applicable in a data-intensive environment where numerical risk assessments are required.

Qualitative approaches, on the other hand, are usually more flexible and adopted by small and medium-sized enterprises (SMEs) which face more strict resource constraints. The methods under this category depend on subjective judgments and often comprise techniques such as holding workshops, interviews, or expert judgments for data collection. The OCTAVE framework [130], for instance, is designed as a self-guided model, enabling organizational teams to carry out internal assessments of security strategies. OCTAVE-S is a variation for smaller organizations' needs; this version has a simpler framework of qualitative analysis. Holistic risk assessments [121] take interdependent risks into account, in particular cascading effects, while event tree analysis [39] systematically maps the potential consequences of events following the initial incidents. Qualitative methods are less technical, hence easier for resource-constrained organizations to undertake. They are, however, less precise compared to quantitative methods.

Hybrid methods combine quantitative and qualitative approaches to build a holistic framework suitable for complex systems. Such methods are more suitable for large organizations where detailed risk assessments need to consider both statistical evidence and qualitative insights. For instance, SecRAM, developed under SESAR SWP16.2 [22], combines probability-impact assessments with the CIA triad, delivering a multi-faceted approach to cyber resilience. The TVRA [117] integrates threat and vulnerability assessment in order to improve the applicability of assessment in complex environments. PASTA [9] and TARA [101] concentrate on structured threat modeling methods to align technical risks with business objectives. Examples of other hybrid approaches are found through the combination of resilience phases and capability maturity assessments via the Cybersecurity Capability Maturity Model C2M2 [117], and the Five-Phase Resilience Assessment Framework [115]. Hybrid methods require cross-disciplinary competencies such as statistical analysis and familiarity with business processes, thus they are applicable in complex and layered organizational structures.

Specialized models are created for specific applications, often in high-impact areas such as CI, safety and security-critical processes, and mission-critical systems. As such, these methods are designed to assess specific types of threats, which often require specialized expertise. One example is the STRIDE threat model [101], which systemically categorizes and models threats in several domains; another example is FAIR [130], which provides a framework for analyzing information risk factors related to cybersecurity. Endsley's Situational Awareness Model [109] formulates awareness levels required to make a decision

in a dynamically changing environment. EVT [20] models extreme cyber risk events, whereas stochastic hybrid models [20] combine stochastic techniques and traditional risk models to cover a broader range of risks. MIPG [131] focuses on the propagation of attacks in complex systems. Specialized models both demand a very high level of technical skills and, in many instances, domain-specific knowledge. The complex nature of these methodologies limits their applicability but provides tailored insights precisely aimed at complex, high-stakes environments.

Table 9. Categorized risk assessment/management methods for resilience enhancement.

Category	Methods
Quantitative Methods	• Probability-impact matrix [22]—Uses probability and impact to assess risks within STRIDE categories. • Risk quantification (TVI) [116]—Calculates risk based on threat, vulnerability, and impact factors. • CVSS [117]—Common vulnerability scoring system; for measuring vulnerability severity. • DREAD [9]—Evaluates threats based on multiple factors. • Vulnerability-Impact-Likelihood [108]—Quantifies risk using vulnerability, impact, and likelihood. • Security Score Model [114]—Quantifies security based on scoring criteria. • CCE scoring method [116]—Used for assessing impact in risk management. • Tail Threshold Detection [20]—Identifies risk event thresholds.
Qualitative Methods	• OCTAVE [130]—OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). This method is usually implemented with qualitative evaluations. • Holistic Risk Assessments [121]—Consider interconnection between risks and emphasize studying cybersecurity risks and the cascading effects. • Event Tree Analysis [39]—Analyzes potential outcomes from initial events. • Direct Testing Method [130]—Uses audits, exercises, and testing. • Raising Awareness [132]—Focuses on cybersecurity awareness among end users.
Hybrid Methods	• SecRAM by SESAR SWP16.2 [22]—Combines probability-impact assessment with CIA triad. • PASTA [9]—Blends qualitative threat modeling with business objectives. • TARA [101]—Uses STRIDE and DREAD to analyze threats. • Cybersecurity Capability Maturity Model (C2M2) [117]—Assesses cybersecurity capabilities. • Five-Phase Resilience Assessment Framework [115]—Quantifies resilience in phases. • Threat, Vulnerability, and Risk Analysis (TVRA) [117]—Combines threat, vulnerability, and risk. • RAMA [110]—Uses probability, impact, historical data, and context for risk analysis. • ICS Cyber Killchain [117]—Assesses risk impact through kill chain analysis. • Logical Attack Graph (LAG) [131]—Visualizes potential attack paths.
Specialized Models	• STRIDE Threat Model [101]—Models threats across various categories. • FAIR [130]—Analyzes information risk factors. • Endsley's Situational Awareness Model [109]—Conceptual model for situational awareness. • Extreme Value Theory (EVT) [20]—Models extreme events in cybersecurity. • Stochastic Hybrid Model [20]—Blends stochastic methods with traditional risk models. • Mission Impact Propagation Graph (MIPG) [131]—Assesses cyber-attack propagation.

5.2. Risk Assessment Standards for Cyber Resilience

The standards and guidelines in the literature on risk assessment for cyber resilience differ in terms of their scope, level of detail, and domain. Some standards are designed to be general and overarching. The most famous guideline in this regard is the NIST CSF, which provides a comprehensive cybersecurity framework that encompasses the entire security life cycle [107,109,113,120,122,124,127,133,134]. The ISO/IEC 27000 series aim to establish the best practices to follow the implementation, maintenance, and management of Information Security Management Systems (ISMSs). The most broadly used standard among the series is ISO/IEC 27001, that provides the process for organizations to adopt an ISMS to systematically and cost-effectively protect their information [107,120,122,130,133].

ISO 27005 provides more detail on information security risk management that supports the ISMS [109,120,122,130,133]. On the other hand, some other standards tighten their focus on risk assessment approaches that can be used in a wide range of domains. In this regard, ISO 31010 is one of the most well-known standards, which guides the selection and implementation of risk assessment techniques [22] that align with the risk management approach outlined in ISO 31000 [117,132]. In addition, NIST SP 800-30 is a prominent risk assessment guideline adopted by several studies for conducting cyber risk assessment for cyber resilience [22,68,108,118,123].

Some other standards and guidelines used in the literature are domain-specific, i.e., they are designed to address the cybersecurity of a specific CI sector. ISO 21434 is a standard for automotive cybersecurity, focusing on the cybersecurity of road vehicles [102]. ISO/SAE 21434 is another standard in this domain, providing guidelines for cybersecurity engineering in road vehicles [39]. In the energy sector, standards and guidelines used by previous studies are IEEE 1547.3 [116], NISTIR [115], IEC 61850 [134], and NERC-CIP [117,119]. Additionally, for maritime transportation, there are IMO MSC.428 (Maritime Cyber Risk Management), IACS E26 and E27, the BIMCO Cyber Security Guidelines, and the Safety4Sea STCW Convention Guidelines [106]. In the emergency sector, the Sendai Framework for Disaster Risk Reduction 2015-2030 and the UN Guidelines on Man-Made and Technological Hazards [121] are mentioned. Moreover, NIST AI RMF is designed for AI-related cyber risks [111] and DO326A/ED-202A provides guidelines for cybersecurity in aviation [22]. Finally, the Cyber Resilience Framework (CRF) and the CERT Resilience Management Model (CERTRMM) provide guidelines for ensuring resilience [9].

Table 10 categorizes various standards, guidelines, and frameworks based on their scope of application, enhancing the understanding of each approach's intended focus.

Table 10. Categorization of risk assessment standards, guidelines, and frameworks based on scope of application.

Scope of Application	Name	Description
System Level	ISO 21434	Targets automotive cybersecurity, providing guidelines for protecting vehicle systems from cyber threats [102].
	IEEE 1547.3	Guides the cybersecurity of distributed energy resources within electric power systems [116].
	IEC 61850	Focuses on communication networks and systems in substations, crucial for electric power system resilience [134].
	DO326A/ED-202A	Provides guidelines for cybersecurity in aviation, protecting aircraft systems from cyber incidents [22].
	NISTIR: Guidelines for Smart Grid Cybersecurity	Addresses cybersecurity issues within smart grid environments [115].
Organizational Level	ISO/IEC 27001	An information security management standard covering a broad range of organizational security aspects [120,133].
	COBIT	Framework for IT governance and management that aligns IT processes with business goals [112].
	NIST Cybersecurity Framework (CSF)	Offers guidelines for CI resilience by establishing security protocols for organizational use [133].
	ISO 31000	General risk management guidelines applicable across organizations for identifying and mitigating risks [117].
	MITRE Framework	Supports threat analysis and mitigation, helping organizations to manage and understand their threat landscapes [129].

Table 10. *Cont.*

Scope of Application	Name	Description
Human-Centric Focus	ENISA Cybersecurity Skills Report	A report by the EU Agency for Cybersecurity aimed at developing essential cybersecurity skills in the EU [110].
	IMO MSC.428	Integrates cyber risk management into maritime operations, focusing on the roles and responsibilities of personnel onboard vessels [106].
	Safety4Sea STCW Convention Guidelines	Provides guidelines for officers with a focus on cybersecurity, emphasizing training and skills needed for cyber resilience in maritime environments [106].

System-level standards, such as ISO 21434 and IEEE 1547.3, focus on securing specific technical systems or sectors, addressing risks directly associated with their operations. These standards play a critical role in safeguarding vital systems in domains like automotive and power systems. Organizational-level standards, including ISO/IEC 27001 and the NIST Cybersecurity Framework, offer a more comprehensive approach by establishing policies, processes, and frameworks for cyber resilience across organizations. These guidelines aid in ensuring that the entire organization, not just isolated systems, adopts a robust cyber resilience posture. Finally, human-centric standards, such as ENISA's Cybersecurity Skills Report and IMO MSC.428, emphasize the significance of human elements in cyber resilience. They target skill development, awareness, and role-specific training to strengthen resilience through an informed and prepared workforce.

5.3. Risk Assessment Governance for Cyber Resilience

One of the most important regulations regarding cybersecurity is the NIS 2 directive [104,109,117,128,132,133]. It is a European Union (EU)-wide legislative act to 'achieve a high common level of cyber security' [145]. NIS 2 will set the baseline for cybersecurity risk management and reporting obligations across a wide range of sectors, including energy, transportation, health, and digital infrastructure [146]. As a compliment to NIS 2 and the EU Cyber Security Act (CSA) [121], the Cyber Resilience Act (CRA) was published to provide essential cybersecurity requirements for all hardware and software products with digital elements [123]. Another very important regulation addressed by studies on cyber resilient risk assessment is the EU General Data Protection Regulation (GDPR), which aims at raising the level of privacy for individuals [109,117,132]. The application of GPDR's requirements is significantly wide and transactional; this means that any sort of process performed on personal data needs to be compliant with it [147].

Similar to standards and guidelines, regulations may also be domain-specific. Particularly, in the maritime sector, the Maritime Safety Management System (SMS) Requirements aim to integrate cyber risk management with maritime SMS [107]. Also, the Certification and Watchkeeping for Seafarers (STCW) is an international convention of general requirements for seafarers, which also includes cybersecurity [107]. In energy, the US Department of Energy Cybersecurity Frameworks provides guidelines for ensuring cybersecurity in the energy sector [131]. In the aviation sector, the International Civil Aviation Organization (ICAO) Aviation Cybersecurity Strategy is designed to manage cybersecurity risks in international civil aviation [105]. In addition, the European Union Aviation Safety Agency (EASA) concept paper outlines the approach to aviation safety and also includes cybersecurity. Moreover, the UN Regulation No. 155 on Cybersecurity focuses on cybersecurity management systems for vehicles in general. The Health Insurance Portability and Accountability Act (HIPPA) governs healthcare data security and privacy in the US healthcare sector [109]. Finally, the EU AI Act is a regulation proposed by the EU to govern AI and its security issues [112].

The review of risk assessment regulations related to cyber resilience shows that although there have been many binding laws and acts to regulate cyber resilience issues, they are not comprehensive enough to manage risks at the organizational level [148]. On

the other hand, cybersecurity regulations are not adequately incentivizing for CI sectors to implement [149].

5.4. Research Limitations

This research acknowledges several limitations and threats to its validity. First, the results of this review are directly influenced by the journal and conference publications included, which could potentially introduce selection bias if relevant studies were missed. We attempted to mitigate this by using a broad, inclusive search strategy, but some relevant work may not be indexed or available in the selected databases. Second, the search string and databases can also influence the results of the review. We tried to use a simple search string and a variety of databases to include as many publications as possible. Further, there is a potential risk of overgeneralization due to the diversity of study contexts and methodologies in the literature. This may pose a threat to internal validity, as diverse approaches may not be directly comparable. To address this, we carefully minimized grouping or categorizing findings.

Moreover, the study faces construct validity limitations, as it relies on definitions and classifications established by prior publications on cyber risk assessment for cyber resilience. Variations in definitions or interpretations of key concepts, such as "cyber resilience", "risk assessment", "governance", and "standards", across studies may affect the comparability of findings. These limitations may be addressed in future research by incorporating expert validation of the review's results, ensuring that the definitions align with current industry and academic standards. Finally, an implementation gap was identified in the review of risk assessment methods for resilience. For instance, ISO 37001:2016 (Anti-bribery Management Systems), highlighted in Table 1 as a highly cited risk management standard, has the potential to enhance cyber resilience by supporting robust internal controls and compliance processes critical for mitigating cyber threats that exploit vulnerabilities arising from corruption. However, no documentation currently demonstrates its use for this purpose. This finding underscores a need for future research to explore the resilience potential of standards and regulations, irrespective of their existing applications.

6. Conclusions

In this study, an SLR on risk assessment for cyber resilience was conducted to investigate related methods, standards, and regulations. The review started with 173 papers, and after the screening process following the PRISMA statement 40 papers were included for a thorough review to extract resilient risk assessment methods, standards, and regulations. The key results of this review are as follows:

- The concept of cyber resilience is relatively young in the context of safeguarding critical systems, and its integration with risk assessment is at its starting stages. This is reflected by the fact that more than half of the papers on this topic have been published only in the past two years.
- Studies that address risk assessment for cyber resilience, focus only on a small number of CI sectors, namely, transportation, energy, healthcare, IT, and emergency services.
- The intersection of risk assessment methods and cyber resilience is continuous monitoring. In order to establish and maintain cyber resilience, cyber risks have to be constantly monitored to identify new threats and vulnerabilities and mitigate the corresponding risks.
- Risk assessment methods for cyber resilience can differ based on how they define risk and which sectors they are designed to cover.
- Cyber resilience in risk assessment standards is often addressed through risk management procedures to realize pre- and post-disturbance protection.
- Although there are some well-designed regulations that cover risk assessment for cyber resilience, such as NIS 2 and CRA, CI sectors are still not motivated enough to implement them.

The SLR in this paper resulted in a comprehensive list of methodologies, frameworks, standards, guidelines, regulations, and legislation in different domains that can support risk assessment from a resilience perspective. They collectively represent the current status of research and practices and can offer researchers a broad perspective on the related knowledge area. Moreover, these lists can provide valuable information for cybersecurity managers, decision-makers, policymakers, and practitioners as a guide to selecting the methods and frameworks and complying with the standards and regulations that are most suitable according to the specific organizational and business features and the sectors in which they operate. Insights derived from the current article support more effective decision making in IT-empowered and cyber-sensitive CI governance. By focusing on key regulatory requirements and best practices, decision-makers can allocate resources more effectively, improving overall organizational resilience. From a strategic point of view, the study highlights the need for standardized cyber resilience practices and increased collaboration among stakeholders. Consequently, the study's findings can help align cyber resilience strategies with both organizational goals and regulatory frameworks, enabling managers to adopt a cohesive approach to managing cyber risks and ultimately enhancing the security and resilience of CI systems.

The categorization of risk assessment methodologies in Section 5.1 brings out the wide range of existing methodologies to enhance resilience. These include quantitative methods, which are especially useful for data-driven organizations; qualitative approaches, which are more suited for smaller companies with limited resources; and hybrid and specialized techniques for complex, critical systems. The method selection depends on an organization's resources, the complexity of its risk environment, and the level of technical expertise available. Moreover, the classification in Section 5.2 reveals the different fields to which standards related to risk assessment apply. This helps organizations to find appropriate standards that match their needs for improving resilience. Knowing the relevant focus areas, organizations can implement targeted strategies toward building resilience against cyber threats at various layers of their operational and technical infrastructure.

For future research, new cyber risk assessment methodologies for cyber resilience may be developed by incorporating cyber resilience factors (e.g., recovery, functionality, adaptability) with probability and impact. Another scope is exploring the combination of multi-criteria decision-making approaches with the existing cyber risk assessment methods for cyber resilience. Finally, several CI sectors have been neglected in the literature of cyber risk assessment for cyber resilience, such as the chemical sector, critical manufacturing, food and agriculture, and water and wastewater. This creates a significant gap in the literature that investigates methods, standards, and regulations for cyber risk assessment for cyber resilience in these CI sectors.

Author Contributions: Conceptualization, M.L.; methodology, A.A.A., M.L. and M.P.; formal analysis, A.A.A. and M.P.; writing—original draft preparation, A.A.A. and M.P.; writing—review and editing, A.A.A., M.L. and M.P.; supervision: M.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used in this study are subject to restrictions. They were obtained from a third party, and due to the sensitive nature of the risk data, they cannot be made publicly available. The company involved in this study has opted not to disclose this information to prevent potential exposure of vulnerabilities.

Conflicts of Interest: Author Ali Aghazadeh Ardebili was employed by the company HSPI SpA-Roma. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Appendix A. Shortlisted Articles

Table A1. Listed articles for full study and information extraction. The ID is used for enumeration and reference within the text.

ID	Ref.	Year	Institutions	Country
Qi1	[129]	2023	Pukhov Institute for Modelling in Energy Engineering "IPME"	Ukraine
Qi15	[133]	2021	Infili Technologies PC, i2CAT Foundation, University of Murcia, ORION Innovations PC, Sfera IT, UBITECH Ubiquitous Solutions, Politecnico di Torino, NEC Laboratories Europe GmbH, inCITES Consulting SA, Hewlett Packard Enterprise, Space Hellas, Stratotiki Sxoli Evelpidon, DBC Europe SA	Greece, Spain, Italy, Slovenia, Germany, Luxembourg, UK
Qi4	[128]	2023	Centre for Cyber Resilience and Trust (CREST)	Australia
Qs59	[117]	2023	University of Warwick, Kohat University of Science & Technology, University of the West of England	UK, Pakistan
Qs63	[118]	2022	Melentiev Energy Systems Institute	Russian Federation
Qs66	[134]	2019	University of Dar es Salaam, Old Dominion University, University of Illinois at Urbana-Champaign	Tanzania, USA
Qs77	[120]	2023	Fraunhofer SIT, ATHENE, Technische Hochschule Mittelhessen	Germany
Qs85	[109]	2024	University of Tras-os-Montes and Alto Douro, University of Aveiro	Portugal
Qs52	[68]	2024	Hansung University, Myongji University	South Korea
Qs84	[104]	2019	Athens University of Economics & Business (AUEB)	Greece
Qs74	[107]	2024	Van Yuzuncu Yıl University, Istanbul Technical University	Turkey
Qs83	[106]	2022	Istanbul Technical University Maritime Faculty, University of Plymouth	Turkey, UK
Qs21	[130]	2022	The University of Indonesia, International Islamic University Malaysia	Indonesia, Malaysia
Qs31	[99]	2018	Thales UK Research Technology and Innovation, Brno University of Technology	UK, Czech Republic
Qs15	[121]	2020	University of Huddersfield School of Art Design and Architecture, United Nations Office for Disaster Risk Reduction New York	UK, USA
Qs20	[114]	2017	Tennessee State University, Old Dominion University	USA
Qs22	[115]	2020	Mississippi State University, US Army Engineer Research Development Center (ERDC)	USA
Qs41	[119]	2024	Hitachi Energy, Iowa State University of Science and Technology	USA
Qs48	[126]	2024	University Of Petra, General Administration Of Electronic Training Institute Of Public Administration, King Abdulaziz University	Jordan, Saudi Arabia
Qs49	[131]	2020	Old Dominion University, U.S. Army Research Laboratory, Crane Division	USA
Qs5	[116]	2021	Idaho National Laboratory, EnerNex, Xanthus Consulting International	USA
Qs26	[110]	2024	SPHYNX Technology Solutions AG, City University of London, University General Hospital of Heraklion	Switzerland, UK, Greece
Qs54	[39]	2023	University of Tras-os-Montes and Alto Douro	Portugal
Qs55	[127]	2021	Università degli Studi di Genova, Università degli Studi di Napoli Federico II	Italy
Qs58	[127]	2024	Z&Co, Murdoch University Dubai, Applied Science Private University	UAE, Jordan
Qs47	[108]	2024	Deakin University, Bangladesh National CERT, King Saud University	Australia, Bangladesh, Saudi Arabia
Qs60	[123]	2024	Leiden University	Netherlands
Qs25	[112]	2024	La Trobe University, Cyberoo Pty Ltd, Massey University	Australia, New Zealand

Table A1. *Cont.*

ID	Ref.	Year	Institutions	Country
Qs64	[113]	2024	Technological University	Ireland
Qs43	[111]	2024	Indiana Tech and Lionfish Cyber Security, Lionfish Cyber Security	USA
Qs2	[102]	2021	Chalmers University of Technology, Volvo Car Corporation	Sweden
Qs40	[101]	2023	Queen's University Belfast	UK
Qs78	[125]	2024	Riga Technical University	Latvia
Qs81	[124]	2024	Institute of Public Administration	Saudi Arabia
Qs23	[22]	2016	Thales UK Limited	UK
Qs35	[105]	2021	Minia University, Nahda University in Beni Suef	Egypt
Qs44	[103]	2023	Queen's University, Institute of Flight Systems	UK, Germany
Qs86	[20]	2023	PRIME RE Solutions, ESPRIT School of Engineering, ESSEC Business School	Switzerland, Tunisia, France
Qs9	[9]	2024	The University of Glasgow, University of Surrey, The University of Auckland	UK, New Zealand
Qw1	[122]	2020	Technical University of Denmark, Man Energy Solutions	Denmark

References

1. Yaacoub, J.P.A.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Malli, M. Cyber-physical systems security: Limitations, issues and future trends. *Microprocess. Microsyst.* **2020**, *77*, 103201. https://doi.org/10.1016/j.micpro.2020.103201.
2. De Felice, F.; Baffo, I.; Petrillo, A. Critical Infrastructures Overview: Past, Present and Future. *Sustainability* **2022**, *14*, 2233. https://doi.org/10.3390/su14042233.
3. Ardebili, A.A.; Padoano, E.; Longo, A.; Ficarella, A. The Risky-Opportunity Analysis Method (ROAM) to Support Risk-Based Decisions in a Case-Study of Critical Infrastructure Digitization. *Risks* **2022**, *10*, 48.
4. Setola, R.; Luiijf, E.; Theocharidou, M. *Critical Infrastructures, Protection and Resilience*; Springer International Publishing: Berlin/Heidelberg, Germany, 2016.
5. Lazari, A. *European Critical Infrastructure Protection*; Springer: Berlin/Heidelberg, Germany, 2014.
6. Araujo, M.S.D.; Machado, B.A.S.; Passos, F.U. Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. *Appl. Sci.* **2024**, *14*, 2116. https://doi.org/10.3390/app14052116.
7. Ardebili, A.A.; Martella, C.; Martella, A.; Lazari, A.; Longo, A.; Ficarella, A. Smart Critical Infrastructures Security management and governance: Implementation of Cyber Resilience KPIs for Decentralized Energy Asset. In Proceedings of the CEUR Workshop—8th Italian Conference on Cyber Security (ITASEC 2024), Salerno, Italy, 8–12 April 2024; Volume 3731.
8. Pettersen, S.; Grøtan, T.O. Exploring the grounds for cyber resilience in the hyper-connected oil and gas industry. *Saf. Sci.* **2024**, *171*, 106384. https://doi.org/10.1016/j.ssci.2023.106384.
9. Alhidaifi, S.M.; Asghar, M.R.; Ansari, I.S. A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions. *ACM Comput. Surv.* **2024**, *56*, 196. https://doi.org/10.1145/3649218.
10. Sharkov, G. From Cybersecurity to Collaborative Resiliency. In Proceedings of the SafeConfig '16: 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense, Vienna, Austria, 24 October 2016; pp. 3–9. https://doi.org/10.1145/2994475.2994484.
11. Björck, F.; Henkel, M.; Stirna, J.; Zdravkovic, J. Cyber resilience–fundamentals for a definition. In *New Contributions in Information Systems and Technologies*; Springer: Berlin/Heidelberg, Germany, 2015; Volume 1; pp. 311–316.
12. Goldman, H.; McQuaid, R.; Picciotto, J. Cyber resilience for mission assurance. In Proceedings of the 2011 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 15–17 November 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 236–241.
13. Petrenko, S. *Cyber Resilience*; River Publishers: Aalborg, Denmark, 2022.
14. Mottahedi, A.; Sereshki, F.; Ataei, M.; Nouri Qarahasanlou, A.; Barabadi, A. The resilience of critical infrastructure systems: A systematic literature review. *Energies* **2021**, *14*, 1571.
15. Osei-Kyei, R.; Tam, V.; Ma, M.; Mashiri, F. Critical review of the threats affecting the building of critical infrastructure resilience. *Int. J. Disaster Risk Reduct.* **2021**, *60*, 102316.
16. Harrop, W.; Matteson, A. Cyber resilience: A review of critical national infrastructure and cyber security protection measures applied in the UK and USA. *J. Bus. Contin. Emerg. Plan.* **2014**, *7*, 149–162.

17. Poulin, C.; Kane, M.B. Infrastructure resilience curves: Performance measures and summary metrics. *Reliab. Eng. Syst. Saf.* **2021**, *216*, 107926.
18. Curt, C.; Tacnet, J.M. Resilience of critical infrastructures: Review and analysis of current approaches. *Risk Anal.* **2018**, *38*, 2441–2458.
19. Aven, T. The Call for a Shift from Risk to Resilience: What Does it Mean? *Risk Anal.* **2019**, *39*, 1196–1203. https://doi.org/10.1111/risa.13247.
20. Dacorogna, M.; Debbabi, N.; Kratz, M. Building up cyber resilience by better grasping cyber risk via a new algorithm for modelling heavy-tailed data. *Eur. J. Oper. Res.* **2023**, *311*, 708–729. https://doi.org/10.1016/j.ejor.2023.05.003.
21. Jacobs, B. A Comparative Study of EU and US Regulatory Approaches to Cybersecurity in Space. *Air Space Law* **2023**, *48*, 477–492.
22. Asgari, H.; Haines, S.; Waller, A. Security Risk Assessment and Risk Treatment for Integrated Modular Communication. In Proceedings of the 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria, 31 August–2 September 2016; pp. 503–509. https://doi.org/10.1109/ARES.2016.6.
23. Lalonde, C.; Boiral, O. Managing risks through ISO 31000: A critical analysis. *Risk Manag.* **2012**, *14*, 272–300.
24. Moeller, R.R. *COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework*; John Wiley & Sons: Hoboken, NJ, USA, 2007.
25. Moeller, R.R. *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes*; John Wiley & Sons: Hoboken, NJ, USA, 2011; Volume 560.
26. Stackpole, C.S. *A User's Manual to the PMBOK Guide*; John Wiley & Sons: Hoboken, NJ, USA, 2013.
27. Ord, T.; Hillerbrand, R.; Sandberg, A. Probing the improbable: Methodological challenges for risks with low probabilities and high stakes. *J. Risk Res.* **2010**, *13*, 191–205.
28. Bier, V.M. Challenges to the acceptance of probabilistic risk analysis. *Risk Anal.* **1999**, *19*, 703–710.
29. Yan, S.; Zhou, X.; Hu, J.; Hanly, S.V. Low probability of detection communication: Opportunities and challenges. *IEEE Wirel. Commun.* **2019**, *26*, 19–25.
30. Ardebili, A.A.; Longo, A.; Ficarella, A. Digital Twins bonds society with cyber-physical Energy Systems: A literature review. In Proceedings of the 2021 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), Melbourne, Australia, 6–8 December 2021; pp. 284–289. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics53846.2021.00054.
31. Kassem, M.A.; Khoiry, M.A.; Hamzah, N. Using probability impact matrix (PIM) in analyzing risk factors affecting the success of oil and gas construction projects in Yemen. *Int. J. Energy Sect. Manag.* **2020**, *14*, 527–546.
32. Aghazadeh Ardebili, A.; Padoano, E. A literature review of the concepts of resilience and sustainability in group decision-making. *Sustainability* **2020**, *12*, 2602.
33. Fraccascia, L.; Giannoccaro, I.; Albino, V. Resilience of complex systems: State of the art and directions for future research. *Complexity* **2018**, *2018*, 3421529.
34. Dvorský, P.; Baštán, O.; Fiedler, P. Complex systems resilience qualification. In Proceedings of the Electrical Engineering, Information and Communication Technologies, EEICT, Brno, Czech Republic, 26 April 2022; pp. 383–387.
35. Zhai, C. Introduction to Complex System Resilience. In *Control and Optimization Methods for Complex System Resilience*; Springer Nature: Singapore, 2023; pp. 1–11. https://doi.org/10.1007/978-981-99-3053-1_1.
36. Werner, M.J.E.; Yamada, A.P.L.; Domingos, E.G.N.; Leite, L.R.; Pereira, C.R. Exploring organizational resilience through key performance indicators. *J. Ind. Prod. Eng.* **2021**, *38*, 51–65.
37. Windle, G.; Bennett, K.M.; Noyes, J. A methodological review of resilience measurement scales. *Health Qual. Life Outcomes* **2011**, *9*, 8.
38. Srinivas, J.; Das, A.K.; Kumar, N. Government regulations in cyber security: Framework, standards and recommendations. *Future Gener. Comput. Syst.* **2019**, *92*, 178–188. https://doi.org/10.1016/j.future.2018.09.063.
39. Pavão, J.; Bastardo, R.; Carreira, D.; Rocha, N.P. Cyber Resilience, a Survey of Case Studies. *Procedia Comput. Sci.* **2023**, *219*, 312–318. https://doi.org/10.1016/j.procs.2023.01.295.
40. *ISO/TS 31050:2023*; Risk Management—Guidelines for Managing an Emerging Risk to Enhance Resilience. International Organization for Standardization: Geneva, Switzerland, 2023.
41. Fahrurozi, M.; Tarigan, S.A.; Tanjung, M.A.; Mutijarsa, K. The use of ISO/IEC 27005: 2018 for strengthening information security management (a case study at data and information Center of Ministry of Defence). In Proceedings of the 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, Indonesia, 6–8 October 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 86–91.
42. Ţigănoaia, B. Some aspects regarding the information security management system within organizations–adopting the ISO/IEC 27001:2013 standard. *Stud. Inform. Control* **2015**, *24*, 201–210.
43. Hendaryatna, H.; Firmansyah, G.; Tjahjono, B.; Widodo, A.M. Performance Evaluation of Business Continuity Plan in Dealing with Threats and Risks in Cilegon Companies Use ISO 22301:2019 & NIST Sp 800-30 R1 Frameworks Case Study: PT. X. *Asian J. Soc. Humanit.* **2023**, *1*, 1159–1174.

44. Ross, R.S. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, 2018. https://doi.org/10.6028/NIST.SP.800-37r2.
45. Ekimova, E.I.; Silaeva, V.V.; Mikhaylov, Y.I. Quality Assurance of Industrial Enterprise Processes Using Risk Identification Methods. In Proceedings of the 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), Saint Petersburg, Russia, 25–28 January 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1650–1653.
46. Crask, J. *Business Continuity Management: A Practical Guide to Organization Resilience and ISO 22301*; Kogan Page Publishers: London, UK, 2024.
47. Mishra, S.; Shukla, V.K. Latest risk management guideline (iso 14971:2019) & environmental aspects of medical device. *Int. J. Drug Regul. Aff.* **2020**, *8*, 15–24.
48. Jun, B.; Kim, J.; Kang, B. A study on the improving ways for effective operation of ISO 37001. *J. Korea Soc. Digit. Ind. Inf. Manag.* **2020**, *16*, 73–82.
49. Prislan, K.; Bernik, I. Risk management with ISO 27000 standards in information security. *Inf. Secur.* **2010**, 58–63.
50. Co, M.; Coleman, C.L.; Davidson, J.W.; Ghosh, S.; Hiser, J.D.; Knight, J.C.; Nguyen-Tuong, A. A lightweight software control system for cyber awareness and security. In Proceedings of the 2009 2nd International Symposium on Resilient Control Systems, Idaho Falls, ID, USA, 11–13 August 2009; pp. 19–24. https://doi.org/10.1109/ISRCS.2009.5251353.
51. Stillman, R.; Defiore, C. Computer Security and Networking Protocols: Technical Issues in Military Data Communications Networks. *IEEE Trans. Commun.* **1980**, *28*, 1472–1477. https://doi.org/10.1109/TCOM.1980.1094838.
52. Dupont, B. The cyber-resilience of financial institutions: Significance and applicability. *J. Cybersecur.* **2019**, *5*, tyz013.
53. Galinec, D.; Steingartner, W. Combining cybersecurity and cyber defense to achieve cyber resilience. In Proceedings of the 2017 IEEE 14th International Scientific Conference on Informatics, Poprad, Slovakia, 14–16 November 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 87–93.
54. Onwubiko, C. Focusing on the Recovery Aspects of Cyber Resilience. In Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 15–19 June 2020; pp. 1–13. https://doi.org/10.1109/CyberSA49311.2020.9139685.
55. Mihalache, S.F.; Pricop, E.; Fattahi, J. Resilience enhancement of cyber-physical systems: A review. In *Power Systems Resilience: Modeling, Analysis and Practice*; Springer: Cham, Switzerland, 2019; pp. 269–287.
56. Bodeau, D.; Graubart, R.; Picciotto, J.; McQuaid, R. *Cyber Resiliency Engineering Framework*; MTR110237; MITRECorporation: Bedford, MA, USA, 2011.
57. Kott, A.; Linkov, I. To improve cyber resilience, measure it. *arXiv* **2021**, arXiv:2102.09455.
58. Bellini, E.; Sargsyan, G.; Kavallieros, D. Cyber-resilience. In *Internet of Things, Threats, Landscape, and Countermeasures*; CRC Press: Boca Raton, FL, USA, 2021; pp. 291–333.
59. Haimes, Y.Y.; Crowther, K.; Horowitz, B.M. Homeland security preparedness: Balancing protection with resilience in emergent systems. *Syst. Eng.* **2008**, *11*, 287–308.
60. Linkov, I.; Kott, A. Fundamental concepts of cyber resilience: Introduction and overview. In *Cyber resilience of systems and networks*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 1–25.
61. Tjoa, S.; Gafić, M.; Kieseberg, P. Standards and Best Practices. In *Cyber Resilience Fundamentals*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 23–35.
62. Brás, J.C.; Pereira, R.F.; Moro, S.; Bianchi, I.S.; Ribeiro, R. Understanding How Intelligent Process Automation Impacts Business Continuity: Mapping IEEE/2755:2020 and ISO/22301:2019. *IEEE Access* **2023**, *11*, 134239–134258.
63. Jovanović, A.; Klimek, P.; Renn, O.; Schneider, R.; Øien, K.; Brown, J.; DiGennaro, M.; Liu, Y.; Pfau, V.; Jelić, M.; et al. Assessing resilience of healthcare infrastructure exposed to COVID-19: Emerging risks, resilience indicators, interdependencies and international standards. *Environ. Syst. Decis.* **2020**, *40*, 252–286.
64. Jovanovic, A.; Renn, O.; Petit, F. Towards more aligned/standardized solutions for indicator-based resilience assessment. *Resilience* **2017**, *2*, 111.
65. Janta, P.; Leeraphun, N.; Thapmanee, K.; Niyomna, P.; Sintuya, H.; Setthapun, W.; Maneechot, P.; Sriprapakhan, P.; Chollacoop, N.; Silva, K. Energy resilience assessment: Incorporating consideration of recoverability and adaptability in risk assessment of energy infrastructure. *Energy Sustain. Dev.* **2024**, *81*, 101506.
66. Proag, V. The concept of vulnerability and resilience. *Procedia Econ. Financ.* **2014**, *18*, 369–376.
67. Ciapessoni, E.; Cirio, D.; Pitto, A.; Sforna, M. A risk-based resilience assessment tool to anticipate critical system conditions in case of natural threats. In Proceedings of the 2019 IEEE Milan PowerTech, Milan, Italy, 23–27 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
68. Park, S.; Park, H. PIER: Cyber-Resilient Risk Assessment Model for Connected and Autonomous Vehicles. *Wirel. Netw.* **2022**, *30*, 4591–4605. https://doi.org/10.1007/s11276-022-03084-9.
69. Chua Chow, C.; Sarin, R.K. Known, unknown, and unknowable uncertainties. *Theory Decis.* **2002**, *52*, 127–138.
70. Dester, W.; Blockley, D. Managing the uncertainty of unknown risks. *Civ. Eng. Environ. Syst.* **2003**, *20*, 83–103.
71. Baltussen, G.; Van Bekkum, S.; Van Der Grient, B. Unknown unknowns: Uncertainty about risk and stock returns. *J. Financ. Quant. Anal.* **2018**, *53*, 1615–1651.

72. Park, J.; Seager, T.P.; Rao, P.S.C.; Convertino, M.; Linkov, I. Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems. *Risk Anal.* **2013**, *33*, 356–367. https://doi.org/10.1111/j.1539-6924.2012.01885.x.
73. Ganin, A.A.; Massaro, E.; Gutfraind, A.; Steen, N.; Keisler, J.M.; Kott, A.; Mangoubi, R.; Linkov, I. Operational resilience: Concepts, design and analysis. *Sci. Rep.* **2016**, *6*, 19540. https://doi.org/10.1038/srep19540.
74. Al-Turkistani, H.F.; AlFaadhel, A. Cyber Resiliency in the Context of Cloud Computing Through Cyber Risk Assessment. In Proceedings of the 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA), Riyadh, Saudi Arabia, 6–7 April 2021; pp. 73–78. https://doi.org/10.1109/CAIDA51941.2021.9425195.
75. Rosato, V.; Pietro, A.D.; Kotzanikolaou, P.; Stergiopoulos, G.; Smedile, G. Integrating Resilience in Time-based Dependency Analysis: A Large-Scale Case Study for Urban Critical Infrastructures. In *Issues on Risk Analysis for Critical Infrastructure Protection*; Rosato, V.; Pietro, A.D., Eds.; IntechOpen: Rijeka, Croatia, 2021; Chapter 5. https://doi.org/10.5772/intechopen.97809.
76. Stergiopoulos, G.; Kotzanikolaou, P.; Theocharidou, M.; Lykou, G.; Gritzalis, D. Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. *Int. J. Crit. Infrastruct. Prot.* **2016**, *12*, 46–60. https://doi.org/10.1016/j.ijcip.2015.12.002.
77. Ale, B.; Burnap, P.; Slater, D. On the origin of PCDS—(Probability consequence diagrams). *Saf. Sci.* **2015**, *72*, 229–239.
78. Tiusanen, R. Qualitative Risk Analysis. In *Handbook of Safety Principles*; Wiley: Hoboken, NJ, USA, 2017. https://doi.org/10.1002/9781119443070.ch21.
79. Anjum, R.L.; Rocca, E. Defining and Assessing Risk. Bias about Values and Probability. In *Philosophy of Science*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 139–159.
80. Hubbard, D.; Evans, D. Problems with scoring methods and ordinal scales in risk assessment. *IBM J. Res. Dev.* **2010**, *54*, 246–255.
81. Woolf*, H. Assessment criteria: Reflections on current practices. *Assess. Eval. High. Educ.* **2004**, *29*, 479–493.
82. Weitz, J. Criteria for criteria. *Am. Psychol.* **1961**, *16*, 228.
83. Wieringa, R.; Maiden, N.; Mead, N.; Rolland, C. Requirements engineering paper classification and evaluation criteria: A proposal and a discussion. *Requir. Eng.* **2006**, *11*, 102–107.
84. Montmain, J.; Labreuche, C.; Imoussaten, A.; Trousset, F. Multi-criteria improvement of complex systems. *Inf. Sci.* **2015**, *291*, 61–84.
85. Voronin, A. *Multi-Criteria Decision Making for the Management of Complex Systems*; IGI Global: Hershey, PA, USA, 2017.
86. Rowe, W.D. Understanding uncertainty. *Risk Anal.* **1994**, *14*, 743–750.
87. Rozet, E.; Marini, R.; Ziemons, E.; Boulanger, B.; Hubert, P. Advances in validation, risk and uncertainty assessment of bioanalytical methods. *J. Pharm. Biomed. Anal.* **2011**, *55*, 848–858.
88. Carot, J.M.; Conchado, A. Detecting measurement biases: Sources of uncertainty, accuracy, and precision of the measurements. In *Imaging Biomarkers: Development and Clinical Integration*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 101–113.
89. Perkins, J.; Suh, S. Uncertainty implications of hybrid approach in LCA: Precision versus accuracy. *Environ. Sci. Technol.* **2019**, *53*, 3681–3688.
90. Maurer, S.D.; Lee, T.W. Accuracy of the situational interview in rating multiple job candidates. *J. Bus. Psychol.* **2000**, *15*, 73–96.
91. Heracleous, C.; Kolios, P.; Panayiotou, C.G.; Ellinas, G.; Polycarpou, M.M. Hybrid systems modeling for critical infrastructures interdependency analysis. *Reliab. Eng. Syst. Saf.* **2017**, *165*, 89–101.
92. Kuhn, A.M.; Youngberg, B.J. The need for risk management to evolve to assure a culture of safety. *BMJ Qual. Saf.* **2002**, *11*, 158–162.
93. Simpson, A.; Murnane, R.; Saito, K.; Phillips, E.; Reid, R.; Himmelfarb, A. *Understanding Risk in an Evolving World: A Policy Note*; World Bank Publications: Washington, DC, USA, 2014.
94. Tranfield, D.; Denyer, D.; Smart, P. Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *Br. J. Manag.* **2003**, *14*, 207–222. https://doi.org/10.1111/1467-8551.00375.
95. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *BMJ* **2021**, *372*, n71. https://doi.org/10.1136/bmj.n71.
96. Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Comput. Ind.* **2018**, *103*, 97–110.
97. Ramirez, R.; Choucri, N. Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review. *IEEE Access* **2016**, *4*, 2216–2243. https://doi.org/10.1109/ACCESS.2016.2544381.
98. Hull, D.; Pettifer, S.R.; Kell, D.B. Defrosting the Digital Library: Bibliographic Tools for the next Generation Web. *PLoS Comput. Biol.* **2008**, *4*, e1000204. https://doi.org/10.1371/journal.pcbi.1000204.
99. Asgari, H.; Haines, S.; Rysavy, O. Identification of Threats and Security Risk Assessments for Recursive Internet Architecture. *IEEE Syst. J.* **2018**, *12*, 2437–2448. https://doi.org/10.1109/JSYST.2017.2765178.
100. Koay, A.M.Y.; Ko, R.K.L.; Hettema, H.; Radke, K. Machine Learning in Industrial Control System (ICS) Security: Current Landscape, Opportunities and Challenges. *J. Intell. Inf. Syst.* **2023**, *60*, 377–405. https://doi.org/10.1007/s10844-022-00753-1.
101. Siddiqui, F.; Khan, R.; Tasdemir, S.Y.; Hui, H.; Sonigara, B.; Sezer, S.; McLaughlin, K. Cybersecurity Engineering: Bridging the Security Gaps in Advanced Automotive Systems and ISO/SAE 21434. In Proceedings of the 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), Florence, Italy, 20–23 June 2023; pp. 1–6. https://doi.org/10.1109/VTC2023-Spring57618.2023.10200490.

102. Strandberg, K.; Rosenstatter, T.; Jolak, R.; Nowdehi, N.; Olovsson, T. Resilient Shield: Reinforcing the Resilience of Vehicles Against Security Threats. In Proceedings of the 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), Helsinki, Finland, 25–28 April 2021; pp. 1–7. https://doi.org/10.1109/VTC2021-Spring51267.2021.9449029.
103. Siddiqui, F.; Ahlbrecht, A.; Khan, R.; Tasdemir, S.Y.; Hui, H.; Sonigara, B.; Sezer, S.; McLaughlin, K.; Zaeske, W.; Durak, U. Cybersecurity Engineering: Bridging the Security Gaps in Avionics Architectures and DO-326A/ED-202A. In Proceedings of the 2023 IEEE/AIAA 42nd Digital Avionics Systems Conference (DASC), Barcelona, Spain, 1–5 October 2023; pp. 1–8. https://doi.org/10.1109/DASC58513.2023.10311187.
104. Lykou, G.; Anagnostopoulou, A.; Gritzalis, D. Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. *Sensors* **2019**, *19*, 19. https://doi.org/10.3390/s19010019.
105. Elmarady, A.A.; Rahouma, K. Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment. *IEEE Access* **2021**, *9*, 143997–144016. https://doi.org/10.1109/ACCESS.2021.3121230.
106. Kayisoglu, G.; Bolat, P.; Tam, K. Evaluating SLIM-based Human Error Probability for ECDIS Cybersecurity in Maritime. *J. Navig.* **2022**, *75*, 1364–1388. https://doi.org/10.1017/S0373463322000534.
107. Soner, O.; Kayisoglu, G.; Bolat, P.; Tam, K. Risk Sensitivity Analysis of AIS Cyber Security through Maritime Cyber Regulatory Frameworks. *Appl. Ocean Res.* **2024**, *142*, 103855. https://doi.org/10.1016/j.apor.2023.103855.
108. Huda, S.; Islam, M.R.; Abawajy, J.; Kottala, V.N.V.; Ahmad, S. A Cyber Risk Assessment Approach to Federated Identity Management Framework-Based Digital Healthcare System. *Sensors* **2024**, *24*, 5282. https://doi.org/10.3390/s24165282.
109. Pavão, J.; Bastardo, R.; Rocha, N.P. Cyber Resilience and Healthcare Information Systems, a Systematic Review. *Procedia Comput. Sci.* **2024**, *239*, 149–157. https://doi.org/10.1016/j.procs.2024.06.157.
110. Smyrlis, M.; Floros, E.; Basdekis, I.; Prelipcean, D.B.; Sotiropoulos, A.; Debar, H.; Zarras, A.; Spanoudakis, G. RAMA: A Risk Assessment Solution for Healthcare Organizations. *Int. J. Inf. Secur.* **2024**, *23*, 1821–1838. https://doi.org/10.1007/s10207-024-00820-4.
111. Jawhar, S.; Kimble, C.E.; Miller, J.R.; Bitar, Z. Enhancing Cyber Resilience with AI-Powered Cyber Insurance Risk Assessment. In Proceedings of the 2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2024; pp. 0435–0438. https://doi.org/10.1109/CCWC60891.2024.10427965.
112. McIntosh, T.R.; Susnjak, T.; Liu, T.; Watters, P.; Xu, D.; Liu, D.; Nowrozy, R.; Halgamuge, M.N. From COBIT to ISO 42001: Evaluating Cybersecurity Frameworks for Opportunities, Risks, and Regulatory Compliance in Commercializing Large Language Models. *Comput. Secur.* **2024**, *144*, 103964. https://doi.org/10.1016/j.cose.2024.103964.
113. Abdi, A.; Bennouri, H.; Keane, A. Cyber Resilience, Risk Management, and Security Challenges in Enterprise-Scale Cloud Systems: Comprehensive Review. In Proceedings of the 2024 13th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 11–14 June 2024; pp. 1–8. https://doi.org/10.1109/MECO62516.2024.10577956.
114. Maziku, H.; Shetty, S. Software Defined Networking Enabled Resilience for IEC 61850-Based Substation Communication Systems. In Proceedings of the 2017 International Conference on Computing, Networking and Communications (ICNC), Santa Clara, CA, USA, 26–29 January 2017; pp. 690–694. https://doi.org/10.1109/ICCNC.2017.7876213.
115. Ibne Hossain, N.U.; Nagahi, M.; Jaradat, R.; Shah, C.; Buchanan, R.; Hamilton, M. Modeling and Assessing Cyber Resilience of Smart Grid Using Bayesian Network-Based Approach: A System of Systems Problem. *J. Comput. Des. Eng.* **2020**, *7*, 352–366. https://doi.org/10.1093/jcde/qwaa029.
116. Culler, M.J.; Morash, S.; Smith, B.; Cleveland, F.; Gentle, J. A Cyber-Resilience Risk Management Architecture for Distributed Wind. In Proceedings of the 2021 Resilience Week (RWS), Salt Lake City, UT, USA, 18–21 October 2021; pp. 1–8. https://doi.org/10.1109/RWS52686.2021.9611786.
117. Mehmood, A.; Epiphaniou, G.; Maple, C.; Ersotelos, N.; Wiseman, R. A Hybrid Methodology to Assess Cyber Resilience of IoT in Energy Management and Connected Sites. *Sensors* **2023**, *23*, 8720. https://doi.org/10.3390/s23218720.
118. Kolosok, I.; Gurina, L. Cyber Resilience Models of Systems for Monitoring and Operational Dispatch Control of Electric Power Systems. *IFAC-PapersOnLine* **2022**, *55*, 485–490. https://doi.org/10.1016/j.ifacol.2022.07.084.
119. Khanna, K.; Govindarasu, M. Resiliency-Driven Cyber–Physical Risk Assessment and Investment Planning for Power Substations. *IEEE Trans. Control Syst. Technol.* **2024**, *32*, 1743–1754. https://doi.org/10.1109/TCST.2024.3378990.
120. Gkoktsis, G.; Lauer, H.; Jaeger, L. Risk Assessments in Virtual Power Plants with NESCOR Criteria, Practical Application, Advantages and Disadvantages. In Proceedings of the 18th International Conference on Availability, Reliability and Security, ARES '23, Benevento, Italy, 29 August–1 September 2023; pp. 1–11. https://doi.org/10.1145/3600160.3605179.
121. Panda, A.; Bower, A. Cyber Security and the Disaster Resilience Framework. *Int. J. Disaster Resil. Built Environ.* **2020**, *11*, 507–518. https://doi.org/10.1108/IJDRBE-07-2019-0046.
122. Sepúlveda Estay, D.A.; Sahay, R.; Barfod, M.B.; Jensen, C.D. A Systematic Review of Cyber-Resilience Assessment Frameworks. *Comput. Secur.* **2020**, *97*, 101996. https://doi.org/10.1016/j.cose.2020.101996.
123. Shaffique, M.R. Cyber Resilience Act 2022: A Silver Bullet for Cybersecurity of IoT Devices or a Shot in the Dark? *Comput. Law Secur. Rev.* **2024**, *54*, 106009. https://doi.org/10.1016/j.clsr.2024.106009.
124. AL-Hawamleh, A. Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security. *Int. J. Comput. Digit. Syst.* **2024**, *15*, 1315–1331. https://doi.org/10.12785/ijcds/150193.

125. Bahmanova, A.; Lace, N. Cyber Risks: Systematic Literature Analysis. In Proceedings of the 15th International Multi-Conference on Complexity, Informatics and Cybernetics, Virtual, 26–29 March 2024; pp. 177–184. https://doi.org/10.54808/IMCIC2024.01.177.
126. Kanaan, A.; AL-Hawamleh, A.; Alorfi, A.; Aloun, M. Cybersecurity Resilience for Business: A Comprehensive Model for Proactive Defense and Swift Recovery. In Proceedings of the 2024 2nd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 26–28 February 2024. IEEE: Piscataway, NJ, USA, 2024; pp. 1–7. https://doi.org/10.1109/ICCR61006.2024.10532881.
127. Itani, D.; Itani, R.; Eltweri, A.A.; Faccia, A.; Wanganoo, L. Enhancing Cybersecurity Through Compliance and Auditing: A Strategic Approach to Resilience. In Proceedings of the 2024 2nd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 26–28 February 2024; pp. 1–10. https://doi.org/10.1109/ICCR61006.2024.10532959.
128. Al-Hawawreh, M.; Doss, R. Enhancing Security in Industrial IoT: A Taxonomy-driven Approach to Risk Assessment. In Proceedings of the 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Exeter, UK, 1–3 November 2023; pp. 434–443. https://doi.org/10.1109/TrustCom60117.2023.00074.
129. Bakalynskyi, O.; Korobeynikov, F. Establishing Goals in the Creation of Cyber-Resilient Systems per NIST. In Proceedings of the 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, 13–15 October 2023; pp. 1–4. https://doi.org/10.1109/DESSERT61349.2023.10416540.
130. Chandra, N.A.; Ramli, K.; Ratna, A.A.P.; Gunawan, T.S. Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools. *Risks* **2022**, *10*, 165. https://doi.org/10.3390/risks10080165.
131. Haque, M.A.; Shetty, S.; Kamhoua, C.A.; Gold, K. Integrating Mission-Centric Impact Assessment to Operational Resiliency in Cyber-Physical Systems. In Proceedings of the GLOBECOM 2020—2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–7. https://doi.org/10.1109/GLOBECOM42002.2020.9322321.
132. Murino, G.; Ribaudo, M.; Romano, S.; Tacchella, A. OT Cyber Security Frameworks Comparison Tool (CSFCTool). In Proceedings of the Italian Conference on Cybersecurity, Online, 8–9 April 2021.
133. Mantas, E.; Papadopoulos, D.; Fernández, C.; Ortiz, N.; Compastié, M.; Martínez, A.L.; Pérez, M.G.; Kourtis, A.; Xylouris, G.; Mlakar, I.; et al. Practical Autonomous Cyberhealth for Resilient Micro, Small and Medium-sized Enterprises. In Proceedings of the 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Athens, Greece, 7–10 September 2021; pp. 500–505. https://doi.org/10.1109/MeditCom49071.2021.9647609.
134. Maziku, H.; Shetty, S.; Nicol, D.M. Security Risk Assessment for SDN-enabled Smart Grids. *Comput. Commun.* **2019**, *133*, 1–11. https://doi.org/10.1016/j.comcom.2018.10.007.
135. Pourmadadkar, M.; Lezzi, M.; Corallo, A. Cyber Security for Cyber-Physical Systems in Critical Infrastructures: Bibliometrics Analysis and Future Directions. *IEEE Trans. Eng. Manag.* **2024**, *71*, 15405–15421 https://doi.org/10.1109/TEM.2024.3489273.
136. Zhou, Y.; Yu, F.R.; Chen, J.; Kuo, Y. Cyber-Physical-Social Systems: A State-of-the-Art Survey, Challenges and Opportunities. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 389–425. https://doi.org/10.1109/COMST.2019.2959013.
137. Shin, J.; Son, H.; Heo, G. Development of a cyber security risk model using Bayesian networks. *Reliab. Eng. Syst. Saf.* **2015**, *134*, 208–217.
138. Lallie, H.S.; Debattista, K.; Bal, J. A review of attack graph and attack tree visual syntax in cyber security. *Comput. Sci. Rev.* **2020**, *35*, 100219.
139. Kathayat, D. International Maritime Organization and Cyber Risk Management Framework. *Supremo Amic.* **2022**, *31*, 67.
140. Ramadan, A.I.H.A.; Ardebili, A.A.; Longo, A.; Ficarella, A. Advancing Resilience in Green Energy Systems: Comprehensive Review of AI-based Data-driven Solutions for Security and Safety. In Proceedings of the 2023 IEEE International Conference on Big Data (BigData), Sorento, Italy, 15–18 December 2023; pp. 4002–4010. https://doi.org/10.1109/BigData59044.2023.10386721.
141. Bank for International Settlements. *Bank for International Settlements*; Bank for International Settlements: Basel, Switzerland, 2024.
142. European Parliament and Council. Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA). *Off. J. Eur. Union* **2022**, L 333. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554 (accessed on 3 September 2024).
143. World Economic Forum. The Cyber Resilience Index: Advancing Organizational Cyber Resilience. World Economic Forum. 2024. Available online: https://www.weforum.org/whitepapers/the-cyber-resilience-index-advancing-organizational-cyber-resilience (accessed on 3 September 2024).
144. Jeimy, J.; Cano, M. FLEXI—A Conceptual Model for Enterprise Cyber Resilience. *Procedia Comput. Sci.* **2023**, *219*, 11–19. https://doi.org/10.1016/j.procs.2023.01.258.
145. EUR-Lex-02022L2555-20221227-EN-EUR-Lex—eur-lex.europa.eu. Available online: https://eur-lex.europa.eu/eli/dir/2022/2555 (accessed on 26 September 2024).
146. Sievers, T. Proposal for a NIS directive 2.0: Companies covered by the extended scope of application and their obligations. *Int. Cybersecur. Law Rev.* **2021**, *2*, 223–231. https://doi.org/10.1365/s43439-021-00033-8.
147. Voigt, P.; von dem Bussche, A. Scope of Application of the GDPR. In *The EU General Data Protection Regulation (GDPR): A Practical Guide*; Voigt, P., von dem Bussche, A., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 9–30. https://doi.org/10.1007/978-3-319-57959-7_2.

148. Adamsky, F.; Aubigny, M.; Battisti, F.; Carli, M.; Cimorelli, F.; Cruz, T.; Di Giorgio, A.; Foglietta, C.; Galli, A.; Giuseppi, A.; et al. Integrated protection of industrial control systems from cyber-attacks: The ATENA approach. *Int. J. Crit. Infrastruct. Prot.* **2018**, *21*, 72–82. https://doi.org/10.1016/j.ijcip.2018.04.004.
149. Chui, K.T.; Gupta, B.B.; Liu, J.; Arya, V.; Nedjah, N.; Almomani, A.; Chaurasia, P. A Survey of Internet of Things and Cyber-Physical Systems: Standards, Algorithms, Applications, Security, Challenges, and Future Directions. *Information* **2023**, *14*, 388. https://doi.org/10.3390/info14070388.