



UNIVERSITY OF  
GLOUCESTERSHIRE

This is a peer-reviewed, final published version of the following document and is licensed under Creative Commons: Attribution 4.0 license:

**Metin, Bilgin, Özhan, Fatma Gül and Wynn, Martin G ORCID:  
0000-0001-7619-6079 (2024) Digitalisation and Cybersecurity:  
Towards an Operational Framework. Electronics, 13 (4226).  
pp. 1-35. doi:10.3390/electronics13214226**

Official URL: <https://doi.org/10.3390/electronics13214226>

DOI: <http://dx.doi.org/10.3390/electronics13214226>

EPrint URI: <https://eprints.glos.ac.uk/id/eprint/14494>

#### **Disclaimer**

The University of Gloucestershire has obtained warranties from all depositors as to their title in the material deposited and as to their right to deposit such material.




The University of Gloucestershire makes no representation or warranties of commercial utility, title, or fitness for a particular purpose or any other warranty, express or implied in respect of any material deposited.

The University of Gloucestershire makes no representation that the use of the materials will not infringe any patent, copyright, trademark or other property or proprietary rights.

The University of Gloucestershire accepts no liability for any infringement of intellectual property rights in any material deposited but will remove such material from public view pending investigation in the event of an allegation of any such infringement.

PLEASE SCROLL DOWN FOR TEXT.

# Digitalisation and Cybersecurity: Towards an Operational Framework

Bilgin Metin <sup>1</sup>, Fatma Gül Özhan <sup>1</sup> and Martin Wynn <sup>2,\*</sup>

<sup>1</sup> Department of Management Information Systems, Bogazici University, Bebek, 34342 Istanbul, Turkey; bilgin.metin@boun.edu.tr (B.M.); ozhanfatma@gmail.com (F.G.Ö.)

<sup>2</sup> School of Business, Computing and Social Sciences, University of Gloucestershire, Cheltenham GL50 2RH, UK

\* Correspondence: mwynn@glos.ac.uk

**Abstract:** As businesses increasingly adopt digital processes and solutions to enhance efficiency and productivity, they face heightened cybersecurity threats. Through a systematic literature review and concept development, this article examines the intersection of digitalisation and cybersecurity. It identifies the methodologies and tools used for cybersecurity assessments, factors influencing the adoption of cybersecurity measures, and the critical success factors for implementing these measures. The article also puts forward the concept of cybersecurity governance process categories, which are used to classify the factors uncovered in the research. Findings suggest that current information security standards tend to be too broad and not adequately tailored to the specific needs of small and medium-sized enterprises (SMEs) when implementing emerging technologies, like Internet of Things (IoT), blockchain, and artificial intelligence (AI). Additionally, these standards often employ a top-down approach, which makes it challenging for SMEs to effectively implement them, as they require more scalable solutions tailored to their specific risks and limited resources. The study thus proposes a new framework based on the Plan-Do-Check model, built around the cybersecurity governance process categories and the three core pillars of governance, culture and standards. This is essentially a bottom-up approach that complements current top-down methods, and will be of value to both information technology (IT) professionals as an operational guide, and to researchers as a basis for future research in this field.



**Citation:** Metin, B.; Özhan, F.G.; Wynn, M. Digitalisation and Cybersecurity: Towards an Operational Framework. *Electronics* **2024**, *13*, 4226. <https://doi.org/10.3390/electronics13214226>

Academic Editors: Aryya Gangopadhyay, Vasile-Daniel Pavaloaia, Rodrigo Martin-Rojas and Piotr Sulikowski

Received: 7 September 2024  
Revised: 17 October 2024  
Accepted: 25 October 2024  
Published: 28 October 2024



**Copyright:** © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

**Keywords:** cybersecurity; digitalisation; digital transformation; critical success factors; cybersecurity adoption factors; cybersecurity governance processes; cybersecurity risk assessment; operational framework

## 1. Introduction

The world has been moving towards digitalisation at an unprecedented pace since the turn of the century. With the rapid advancements in technology, businesses are increasingly adopting digital processes and solutions, transforming how they conduct business to increase their efficiency and productivity in an ever more competitive environment [1]. There is an immense reliance on digitalisation in every aspect of the business world through technologies like Internet of Things (IoT), artificial intelligence (AI), machine learning (ML), cloud computing, blockchain, digital twins, and the glue that holds all of these together: the internet. This inevitably brings many new challenges for businesses, with cybersecurity threats and attacks being one of the most prominent. Especially with the COVID-19 pandemic, companies have had to adjust their businesses for remote operations and home offices for employees, which led to an increase in digital processes and practices and the use of diversified mobile devices, creating new vulnerabilities for businesses [2].

Cybersecurity is an evolving field and has no universally agreed definition. Based on a semantic analysis of 28 cybersecurity definitions, Schatz et al. [3] (p. 66) defined cybersecurity as “the approach and actions associated with security risk management processes followed by organisations and states to protect the confidentiality, integrity, and availability of data and assets used in cyberspace”. It involves tools and techniques to

protect companies from cyber threats and business disruptions [4]. As noted by several researchers, cybersecurity threats include data breaches, system disruptions through cyber-attacks leading to business discontinuity [5], financial threats [6], breach of intellectual property [7], loss of trust and reputation public safety issues such as attacks on autonomous vehicles (AV) or food industries [7], and violation of the General Data Protection Regulation (GDPR) [8].

Cyber risk, on the other hand, pertains to the operational risks of economic losses due to the unavailability, lack of integrity, or confidentiality breaches of data and information systems [8]. Effective cybersecurity measures help prevent unauthorised access, data breaches, and other malicious activities that can disrupt operations and lead to significant financial and reputational damage.

This article comprises five sections. Following this brief introduction, Section 2 provides an overview of some key aspects of cybersecurity, outlines a conceptual framework based on cybersecurity governance process categories, and poses four research questions for the study. Section 3 then sets out the research methodology, based on a systematic literature review. In Section 4, the results of the study are presented, directly addressing the four research questions, including the presentation of the new cybersecurity framework, of particular relevance to small and medium-sized enterprises (SMEs) with limited resources. Finally, Section 5 provides some conclusions to the study, notes its limitations and its contribution, and points out possible areas for future research.

## 2. Business Cybersecurity and the Conceptual Framework

Digital transformation is a way for businesses to transition their business processes to IT solutions that deploy digital technologies. While such technological advances offer productivity benefits, they also necessitate a “reorientation of risk analysis and required security measures” [9] (p. 1). Companies need to balance the adoption of new technologies with corresponding cybersecurity measures to address new types of risks and fully benefit from digital transformation [5]. Consumers highly value the security of their personal data, and due to the possibility of violating consumer trust as a result of data or security breaches, businesses must ensure that any process digitalisation they undertake addresses cybersecurity risks and takes the necessary protective measures. Implementing robust cybersecurity measures ensures that these digital processes are secure, protecting sensitive information and maintaining the integrity of operations. This not only enhances the resilience and continuity of business activities but also builds trust with customers and stakeholders.

The protection of sensitive data, maintaining operational continuity, mitigation of financial risks, preventing reputational damage and loss of customer trust, compliance with regulations, and ability to securely adapt to technological advancements are identified as the primary contributions of cybersecurity to business process digitalisation in the extant literature, and there are a range of examples from different sectors in the literature. For example, in the insurance sector, the business relies on customers’ PII (Personal Identifiable Information) as well as their financial information, and recent research [8] pointed out that although cybersecurity investments do not seem to have a direct impact on the company’s profits, they are crucial for the existence of the company. Cybersecurity measures protect the company against loss of business, and its reputation, as well as against legal fees arising from laws and regulations due to data breaches or system shutdowns.

Digitalisation may necessitate the use of IoT devices. Rizvi et al. [10] discuss the growing use of IoT devices in enterprises in the manufacturing, healthcare, and finance sectors, and the security challenges they pose. They propose a modular IoT auditing framework specifically for IoT environments, complete with a set of auditing questions for all security-related features of IoT devices and accompanied by examples and case studies. In their study, they focus on the unique vulnerabilities of IoT devices that make them more susceptible to cyber threats compared to traditional IT systems and remark that proper cybersecurity measures can help protect these devices, and therefore the business processes that rely on the data collected by them. IoT devices often collect and transmit

vast amounts of sensitive data. For instance, in manufacturing, they can be used to monitor equipment performance, predict maintenance needs, optimise production schedules; in healthcare, they can be used as wearable IoT devices to monitor patient health and transmit that data to healthcare professionals; in finance, they can be used for financial transactions. Considering such highly critical use of IoT devices, ensuring their security is critical for protecting the confidentiality, integrity, and availability of data. Furthermore, if IoT devices are not secured properly, they can easily become gateways for cyber attackers aiming to compromise an organisation's IT infrastructure or damage the operations or reputation of a company [10].

In a study investigating the factors that differentiate SMEs in Thailand in terms of adopting or not adopting cybersecurity standards using a quantitative approach, Auyporn et al. [11] surveyed SME IT leaders to assess various cybersecurity adoption factors. They point out that SMEs are often more vulnerable to cyberattacks due to limited resources and less robust cybersecurity measures compared to larger organisations. They highlight the role that SMEs often play as vendors or partners to larger organisations and draw attention to how lack of proper cybersecurity in SMEs' business processes can lead to negative consequences for broader business ecosystem by explaining how SMEs can become gateways for cyber attackers to attack larger organisations that those SMEs work with. Through a survey of cybersecurity in the Swedish manufacturing industry, Franke and Wernberg [5] identified business interruption as the most severe kind of cybersecurity incident based on the answers of the surveyed participants. As manufacturing increasingly depends on digital technologies, a cyberattack on the manufacturing companies' digital processes and technologies could easily halt their operations, causing huge financial losses.

Bui et al. [6] discussed digitalisation in agriculture, i.e., Agriculture 4.0, and how it escalated cybersecurity risks in the sector. The authors of the paper explained how smart farming technologies and infrastructure have become a target for cyber attackers and highlighted the importance of implementing robust cybersecurity measures to safeguard the food supply chain. According to the authors, the risks associated with not having strong cybersecurity defences in the agricultural sector include false data injections via IoT devices leading to data driven decision errors, resource misallocation, disruption in the supply chain; side-channel attacks aiming to access sensitive information; distributed denial-of-service (DDoS) attacks causing disruptions in the normal operations of businesses and so on. In a similar vein, Alqudhaibi et al. [7] discussed the cybersecurity risks arising from the food industry's digitalisation. The negative outcomes of not having strong cybersecurity in business processes as well as systems and devices used in the food industry can have severe impacts on the entire food chain.

In a study discussing the possible benefits of maritime digitalisation using the "concept of DigiShip", Yue et al. [12] conducted a case study on the remote connection of a tugboat in the coastal waters of Singapore. In their study, they carried out cybersecurity threat modelling and risk assessment using STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege) and HEAVENS (Healing Vulnerabilities to Enhance Software Security and Safety) methodologies, respectively. According to the authors, "one of the key systems onboard a vessel that could be of interest to malicious hackers, and vulnerable to cyber security attacks is the system that controls the platform systems onboard the vessel" [12] (p. 4).

As can be seen from these examples, no sector or industry is exempt from the risks arising from not having strong cybersecurity measures integrated into business processes and systems. Therefore, while acknowledging the advantages that digitalisation brings, digitalisation efforts should always be carried out taking cybersecurity into consideration. This was emphasised by Obwegeser et al. [13] (para. 3) who concluded, "the reality for many organisations is that digital transformation consists of an ungainly confederacy of digital initiatives revolving around new technologies, a few Skunk Works projects, and random acts of digital enablement".

Process management is a systematic approach to making an organisation's workflow more effective, more efficient and more capable of adapting to an ever-changing environment [14]. More specifically, process mapping and process analysis have been used in many areas of research related to information technology implementation. These include analysis of information systems in both large companies [15] and SMEs [16] as well as in higher education [17] (Figure 1).



**Figure 1.** Process mapping at a major oil company. Based on: [15].

However, process definition is not an exact science and is to some extent a subjective exercise. Senkus et al. [18], in their critical literature review of process definitions, concluded “the analysis of literature sources showed many definitions of the process, but there is no holistic approach” (p. 242), and the process labels depicted in Figure 1 represent just one approach in a particular business context. Whilst there is a substantial amount of research in the literature that looks into different aspects of cybersecurity related issues and practices, the number of studies that approach the topic from the perspective of processes remains limited. Amongst these few studies, Franke and Wernberg [5] suggested focussing on different process areas, in which different types of cyber risks with different security measures could be identified and implemented. They highlighted the gap between the estimated impact of digitalisation and the need for cybersecurity measures within different processes. They suggested investigating the relationship between digital and cybersecurity maturity to address different security needs, differentiating security measures for various types of cyber risks, and balancing technology related measures with social (human) and organisational security aspects. In addition, Bechara and Schuch [19] highlight the significance of regulatory measures in cybersecurity management that requires an external focus, whilst NordLayer [20] associate cost and resource provision with having an internal process focus. Ogono [21] offers a definition of cybersecurity processes as “the requirements and steps that cyber security analysts implement as they execute their duties. These processes may vary slightly across cyber security firms but the goal is usually the same—to prevent and defend against cybercrime” (para. 12). However, the identified processes are more stages for the identification, protection, monitoring and recovery of assets, rather than the type of process discussed here.

The term “cybersecurity governance process categories” is used here to mean “processes that support the planning, implementation and maintenance of cybersecurity, which interact with standard business processes, but which comprise a series of factors rather than activities”. Five governance process categories are recognised—human, external, finan-

cial, technological, and organisational (Table 1)—that provide the conceptual framework (Figure 2) for the analysis of the literature examined in this study, and is evidenced in particular in addressing research questions 2 and 4 noted below. One point to note is that an organisation’s compliance with external regulations, and its oversight of third-party suppliers, are both seen as elements of the external factor, because both are influenced by developments beyond the organisation’s immediate control. External regulations and industry standards impact the organisation and its suppliers. Ensuring third parties comply with these standards is crucial to maintaining cybersecurity integrity across the entire supply chain, and underscores the significance of third-party vulnerabilities and their potential impact on the organization. Regulatory measures and cost and resource provision are particularly related to, and aligned with, cybersecurity governance. They serve as guiding constraints that influence the design and operation of secure digital business processes.

**Table 1.** Cybersecurity governance process categories descriptions.

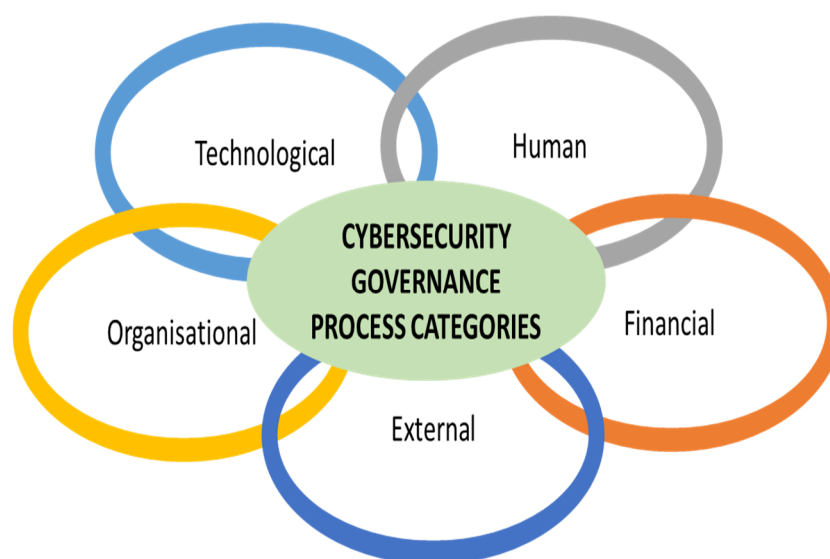
Process Category	Description
External	External process factors relate to the outside regulations, industry standards and best practices that affect the decisions of an organisation regarding cybersecurity adoption. In terms of implementation critical success factors (CSFs), they are about ensuring robust cybersecurity not only within the company but also in the 3rd parties that the organisation is associated with in order to ensure all round comprehensive protection.
Financial	Financial resources are a key determinant in a company’s ability to invest in cybersecurity measures. The financial adoption factors and implementation CSFs that fall under this category relate to an organisation’s financial capacity to (1) implement cybersecurity measures and (2) sustain the implemented measures successfully.
Human	This process category concerns the human factors that play a critical role in the successful adoption and integration of cybersecurity measures. For instance, without adequate security awareness among employees, phishing attempts or social engineering attacks may succeed from the threat point of view. Similarly, without the necessary awareness of employees, any technical cybersecurity measure that is implemented may fail to be effective from the security control point of view.
Organisational	This process category concerns factors related to aspects like business continuity, company reputation, customer needs, and cybersecurity governance. The organisational process category is particularly wide and multi-faceted and impacts right across business functions.
Technological	This involves the technology related issues that impact decision-making relating to cybersecurity adoption and implementation. It thus encompasses the technology aspects of decisions regarding the acquisition and deployment of cybersecurity tools and systems, and their on-going maintenance. It also encompasses cybersecurity assessment of the wider company IT portfolio.

The conceptual framework for the study was distilled from the existing literature and builds upon process definitions found in other sources noted above. Miles and Huberman [22] point out that the conceptual framework “explains, either graphically or in narrative form, the main things to be studied—the key factors, constructs or variables- and the presumed relationships among them” (p. 18). In similar vein, Loaiza et al. [23] note: “a conceptual framework is an analytical tool that studies different concepts. It allows researchers to make comparisons and organize ideas. It not only gathers concepts, but also integrates them into one single structure” (p. 7). So here the framework, depicted in Figure 2, provides the platform upon which the subsequent data analysis and the development of the operational model are undertaken, as discussed below in Section 4. This article thus includes a focus on



the factors that influence businesses in adopting cybersecurity measures, and investigates how these measures can best be integrated into digitalisation at process level, using the five-way cybersecurity governance process categories noted above. More specifically, the study addresses four research questions (RQs):

- RQ1. What are the methodologies and tools that organisations use when conducting cybersecurity assessments associated with process digitalisation?
- RQ2. What factors influence the adoption of cybersecurity measures in digital transformation, and what are the critical success factors (CSFs) during and after the implementation of those cybersecurity measures?
- RQ3. What industry standards/frameworks, and regulations are of significance for cybersecurity in the context of digital transformation?
- RQ4. What new cybersecurity framework can be developed to coordinate guidelines, strategies, and standards specifically for SMEs to complement current top-down perspectives?



**Figure 2.** The five cybersecurity governance process categories used as a conceptual framework in the study.

### 3. Research Method

To address the RQs noted above, key literature was first examined and analysed. A systematic literature review (SLR) identified 34 studies of particular relevance. As Kitchenham and Charters noted in [24] (p. vi), “a systematic review is a means of evaluating and interpreting all available research relevant to a particular research question, topic area, or phenomenon of interest. Systematic reviews aim to present a fair evaluation of a research topic by using a trustworthy, rigorous, and auditable methodology”. SLRs can help both researchers in academia and practitioners from the business world to access synthesised diverse findings on a given topic. In this research, the systematic approach adopted by Niknejad et al. [25] was used, in which the researchers make use of the review process outlined in Kitchenham and Charter’s [24] SLR guidelines. The following sections detail the steps in this process.

#### 3.1. Review Protocol

Having a review protocol helps minimise researcher bias and prevents the research from losing its focus. It also offers the possibility for other researchers to check the validity of an SLR by repeating the steps identified in the review protocol. The study uses the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) protocol [26], which is depicted as applied in this study in Figure 3. The steps in the PRISMA protocol help

determine the RQs, the search strings, the inclusion and exclusion criteria, executing search string, selecting articles, extracting data from the articles, synthesising the data and analysing the results, and finally, writing the report.

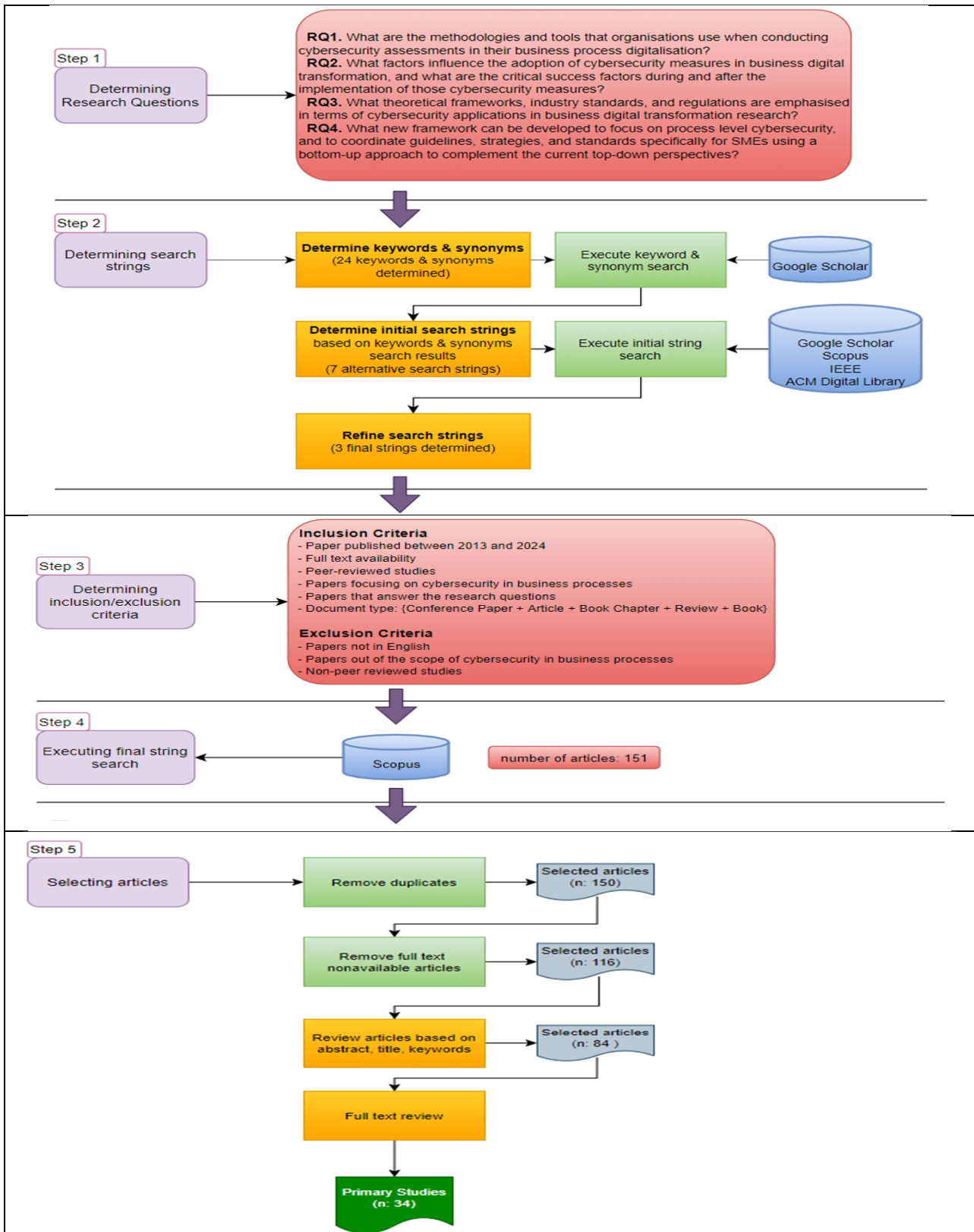
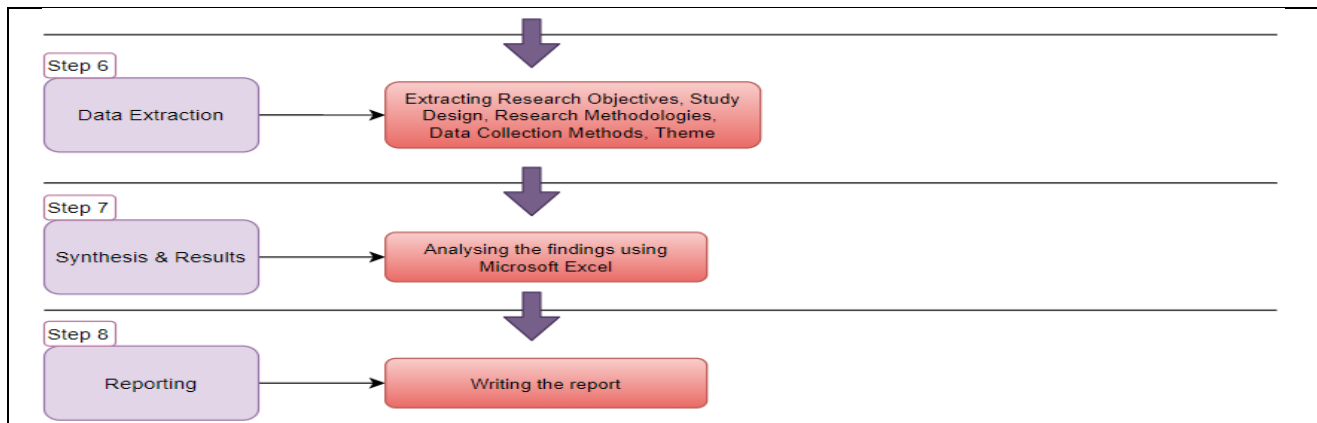


Figure 3. Cont.





**Figure 3.** Application of the PRISMA review protocol in this study.

### 3.2. Inclusion and Exclusion Criteria

Inclusion and exclusion criteria are indispensable to an SLR. These criteria help researchers ensure relevance among the selected articles, maintain consistency throughout the research process, manage scope, increase the transparency and reproducibility of a research, and avoid researcher bias. In line with the focus of the study, which is to review the business process cybersecurity research in the literature, the articles selected in this SLR include articles, conference papers, books, book chapters, and reviews in English published between 2013 and 2024. The year 2013 was selected as it is the year that the second version of the Information Security Management Standard (ISO 27001:2013) was published. This was a significant update from the previous ISO/IEC 27001:2005 version [27]. ISO/IEC 27001:2005 (Clause 4.2.1) presented an asset-based risk assessment approach, focusing on identifying risks against specific assets, with asset owners responsible for determining risk treatment. This method emphasised asset protection over integrating information security into broader business processes, often leading to a checklist-driven mentality. In contrast, the 2013 revision shifted to a process-based risk management approach aligned with ISO 31000:2009 [28], assessing risks in relation to the organization's overall business objectives. This was subsequently superseded by a later version ISO 31000:2018 [29].

This change required organisations to adopt a more holistic and proactive approach to cybersecurity, integrating it closely with business processes and strategic goals. New clauses in ISO/IEC 27001:2013, such as Clause 4 on organisational context and Clause 4.2 on interested parties, expanded the strategic context of information security to include stakeholders, business functions, and external parties. Furthermore, Although ISO/IEC 27001:2005 and earlier standards such as BS 7799 [30] laid the foundation for information security management systems, their focus was more on general information security controls rather than on the integration of cybersecurity into business processes. These changes in ISO/IEC 27001:2013 encouraged organisations to consider how information security impacts the entire organization, not just technical assets. Starting the review from 2013 allowed the capture of these significant shifts in how organisations approach cybersecurity, reflecting a pivotal change in both research and practice, emphasizing the integration of cybersecurity into broader organisational strategies. Although a newer version of this international standard was published in 2022, selecting 2022 as the starting point would considerably limit the articles in the literature review. The full list of inclusion and exclusion criteria can be seen in Table 2.

**Table 2.** Research inclusion and exclusion criteria.

Criteria	Principle
Inclusion	Papers published between 2013 and 2024 Full text availability Peer-reviewed studies Papers focusing on cybersecurity in business processes Papers that answer the research questions Document type: {Conference Paper + Article + Book Chapter + Review + Book}
Exclusion	Papers not in English Papers out of the scope of cybersecurity in business processes Non-peer reviewed studies

### 3.3. Search Strategy

As part of establishing the search strategy, 24 different keywords, and their synonyms, relevant to the topic of cybersecurity in business processes were identified. The base terms used were “business”, “process”, “digitalisation”, and “cybersecurity”; these were alternatively combined with words like “assessment”, “measures”, “models” and so on. The 24 keywords and synonyms were then searched on Google Scholar to see which keywords yielded the most results. The ones that produced the most results were selected for string search formation; others were eliminated. Combining the keywords selected in the previous step in alternative ways like shifting word orders or replacing some words with other keywords or removing some of the words, 7 search strings were determined. These were then used to search for articles on online academic databases Google Scholar, Scopus, IEEE Xplore Digital Library, and ACM Digital Library. This was also a trial step for optimising the search strings by examining the number of results returned on each database for the 7 search strings. Following this optimisation step, 3 final search strings were determined. The researchers tried further reducing the number of search strings by combining them in alternative ways; however, none of the combinations yielded enough articles to work with. As a result, it was decided to use 3 separate search strings. Each of these focuses on a different aspect of this review paper’s research topic.

- Search String 1: (“cybersecurity” OR “cyber security”) AND (“critical success factors” OR “success factors” OR “significant factors” OR “influential factors”)
- Search String 2: (“business processes” OR “digital transformation” OR “digitalisation”) AND (“security evaluation” OR “security auditing” OR “security assessment”)
- Search String 3: (“business processes” OR “digital transformation” OR “digitalisation”) AND (“adoption” OR “adopting” OR “implementation” OR “implementing”) AND (“cybersecurity measures” OR “cyber security measures”)

To execute these final search strings, Elsevier’s Scopus database was used, which is the largest and most reliable online database for peer-reviewed papers. The search results for these 3 strings are presented in Appendix B Table A2.

By applying the search strategy noted above, 151 papers of relevance to the study at hand were located. Following removal of duplicates and papers without full text availability, 116 papers were left for initial review based on title, abstract and keywords. 32 of these papers were deemed unrelated based on the inclusion and exclusion criteria and were eliminated. A detailed full text review was conducted on the remaining 84 papers, and of these, 50 were eliminated based on the inclusion and exclusion criteria set out above. Finally, 34 primary studies remained (see Appendix A Table A1).

### 3.4. Data Extraction and Synthesis

The 34 primary papers were studied carefully and material relevant to the 4 research questions was meticulously recorded. Metadata was extracted from the Scopus database and information about the research topic in each of the studies was collected after reading

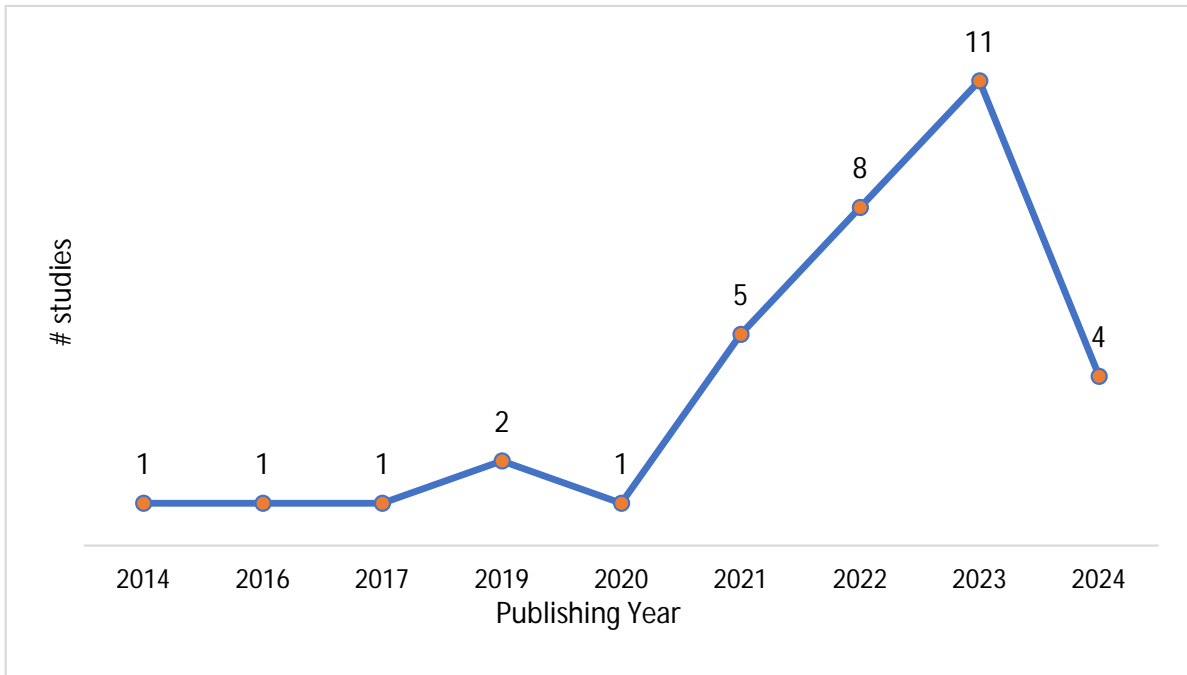
each article, and this was stored in Microsoft Excel sheets (Microsoft 365 MSO Version 2402) to create the data extraction forms. The columns in the data extraction forms are shown Table 3.

**Table 3.** Data extracted from primary studies.

Extracted Data	Description
Paper ID	A unique number assigned to each primary study
Related RQs	Shows the research question(s) that primary papers answer
Title	Title of the paper as displayed in Scopus search results
Author(s)	Author name(s)
Year	The publication year of the paper
Objective	The main objective of the reviewed primary papers
Research strategy	Case study, conceptual study, survey, interview, systematic literature review etc.
Methodology	Qualitative, quantitative, mixed method
Data collection method	Survey, interview, literature review, documentation, observation etc.
Subject	Data collection subjects such as interview and survey participants or papers in a literature review
Country/Region	The specific country or region that the reviewed paper focuses on
Online database/publisher	Where the paper was published
Document type	Article, conference paper, review
Publication source	Journal, conference proceedings etc.
Journal/Conference Name	Name of the conference or journal where the paper was presented or published
Cybersecurity theme	The main focus of the study: cybersecurity assessment, cybersecurity auditing, cybersecurity management, cybersecurity adoption/implementation
Assessment tools and methodologies (RQ1)	The tools and methodologies used in cybersecurity assessment of business processes
Adoption factors/integration CSFs (critical success factors) (RQ2)	The factors affecting the adoption or successful integration of cybersecurity measures in business processes
Cybersecurity Standards/Frameworks & Regulations (RQ3)	The international standards, regulations as well as widely used industry frameworks suggested or adopted by the reviewed primary papers
Gaps, limitations, and future work recommendations	The gaps, limitations, and future work recommendations extracted from the reviewed primary articles

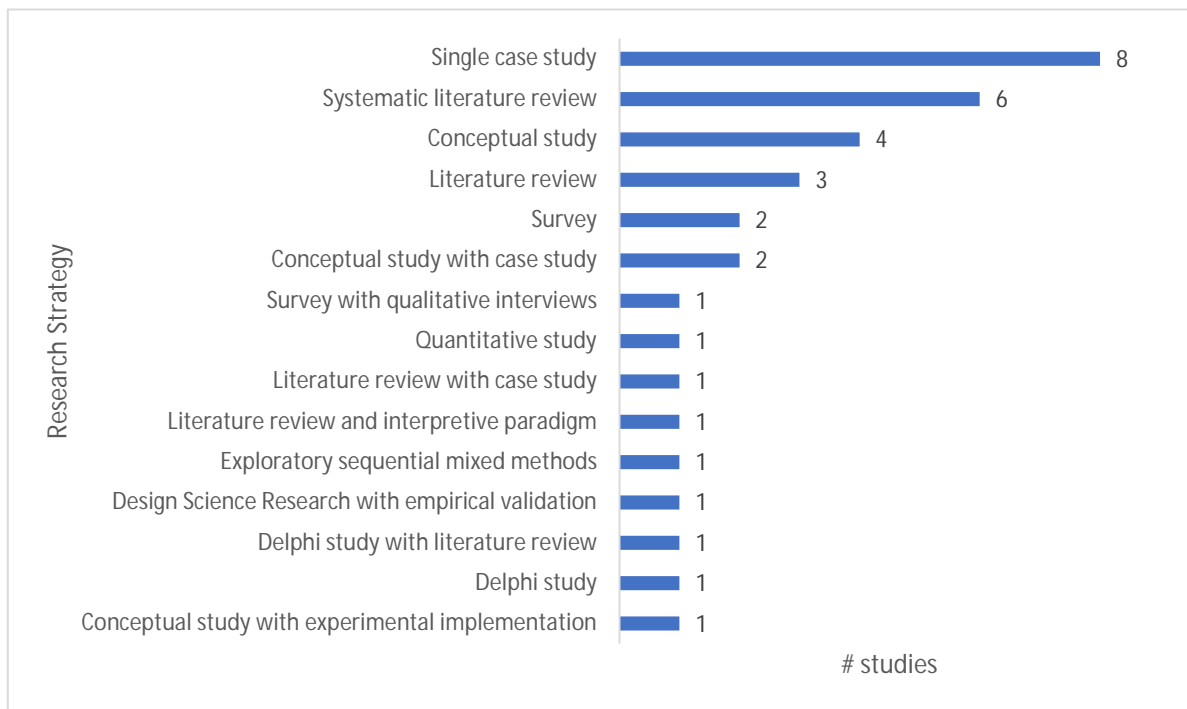
Of the 34 primary papers, 18 (53%) were articles, 13 (38%) were conference papers, and 3 (9%) were reviews. The full names of the conferences and journals are provided in Appendix C Table A3.

The study only considered papers published between 2013 and the end of May 2024, and out of the 34 papers studied, more than half (68%) are from the last 3 years (Figure 4).



**Figure 4.** Temporal view of the primary papers.

As regards the research methodology used in these studies, 26 (76%) of the papers employed a mixed methods approach while 5 (15%) of them were qualitative and 3 (9%) were quantitative. There was a greater diversity in the research strategies adopted in these papers, with a single case study strategy (8 papers) and systematic literature reviews (6 papers) being the most common (Figure 5), Appendix B Table A2 presents the research strategies employed by each primary paper along with the research methodologies and data collection methods.



**Figure 5.** Distribution of research strategies.

The reviewed papers were also classified according to the primary theme of each paper. 4 primary themes were identified: cybersecurity assessment; cybersecurity auditing; cybersecurity management; and cybersecurity adoption/implementation. The definitions of these themes and the primary papers that fall under each theme are shown in Table 4. 16 primary papers (47%) focused on the theme of Cybersecurity Management, whilst 10 primary papers (29%) focused specifically on the theme of Cybersecurity Assessment. Of the 6 papers (18%) focusing on cybersecurity adoption/implementation, some discuss the factors that affect the adoption of cybersecurity measures in business processes while others examine the success factors during and after the implementation of cybersecurity measures in business processes. Even though the papers were divided into these overall themes based on what they are primarily focused on, most of them also provide answers for other themes. For instance, the primary theme of the paper written by Hidayat and Wang [8] is cybersecurity assessment as it primarily aims to assess the operational effectiveness of implemented cybersecurity measures at an Indonesian Life Insurance company; however, the paper also provides insights into the theme of cybersecurity adoption/implementation by listing some factors that have an impact on the adoption of cybersecurity measures such as top management support and regulatory compliance.

**Table 4.** List of cybersecurity themes, their definitions, and the related primary papers.

Cybersecurity Primary Theme	Explanation of the Theme	Related Primary Paper
Cybersecurity assessment	Involves evaluating the current security posture, identifying vulnerabilities, and assessing risks	P1, P11, P12, P13, P17, P19, P20, P24, P28, P32
Cybersecurity auditing	Ensures compliance with internal and external standards, procedures and regulations through audits, reviews, and evaluations of business processes and security controls. Includes penetration testing, security audits, and compliance checks	P2, P22
Cybersecurity management	Deals with the strategic and operational management of cybersecurity within an organisation. Focuses on which cybersecurity measures to be taken, how to manage them, the success or failure of cybersecurity measures and so on	P5, P6, P9, P10, P14, P15, P16, P18, P21, P23, P25, P26, P27, P29, P31, P34
Cybersecurity adoption/implementation	Related to the factors that influence the adoption of cybersecurity practices in business processes as well as the critical success factors during and after the implementation of cybersecurity measures	P3, P4, P7, P8, P30, P33

#### 4. Results

This section addresses the four RQs set out in Section 2.

##### 4.1. RQ1. What Are the Methodologies and Tools That Organisations Use When Conducting Cybersecurity Assessments Associated with Process Digitalisation?

Out of the 34 primary papers, 16 of them provided various suggestions for methodologies to be used in cybersecurity assessment while 5 papers made suggestions about the use of assessment tools Table 5. There is not always a clear distinction between tools and methodologies, and they are sometimes part of the overall assessment and audit process. For instance, Yue et al. [12] used the HEAVENS risk assessment methodology together with STRIDE, a threat modeling tool by Microsoft.

**Table 5.** Primary papers associated with each assessment tool and methodology.

<b>Cybersecurity Assessment Methodology (16 unique papers)</b>	<b>Primary Paper ID</b>
Control Frameworks	P2, P28, P34
Penetration Testing	P8, P17, P19, P34
Risk Assessment and Compliance Frameworks	P1, P2, P8, P9, P11, P12, P13, P15, P17, P18, P19, P20, P22, P32, P34
Threat Intelligence	P34
Threat Modelling	P8, P11, P18, P32
<b>Cybersecurity Assessment Tool (5 unique papers)</b>	
Monitoring Systems (SIEM, IDS/IPS, DLP, Threat Intelligence)	P1, P34
Vulnerability Scanners (Nessus, OpenVAS, OWASP ZAP, Metasploit, Nmap)	P17, P19, P32

As regards specific methodologies and tools, 15 out of the 34 primary papers suggested various Risk Assessment and Compliance Frameworks. For instance, Hidayat and Wang [8] used the National Institute of Standards and Technology (NIST) Cybersecurity Framework (version 1.1) to assess the maturity level of an Indonesian Life Insurance Company's existing cybersecurity measures. Chobanov [31] noted that standards like ISO/IEC 27005 [32], ISA/IEC 62443 [33], or NIST SP 800-82 [34], which are primarily intended for industrial control systems, are also being used in the energy sector.

4 papers proposed Penetration Testing as an assessment methodology. For instance, Alqudhaibi et al. [7] highlighted the criticality of detecting anomalies in the network or system through penetration tests. However, in an online survey they conducted as part of their research to assess the UK food industry's current state of cybersecurity, they found that only 25% of the surveyed companies carried out penetration tests.

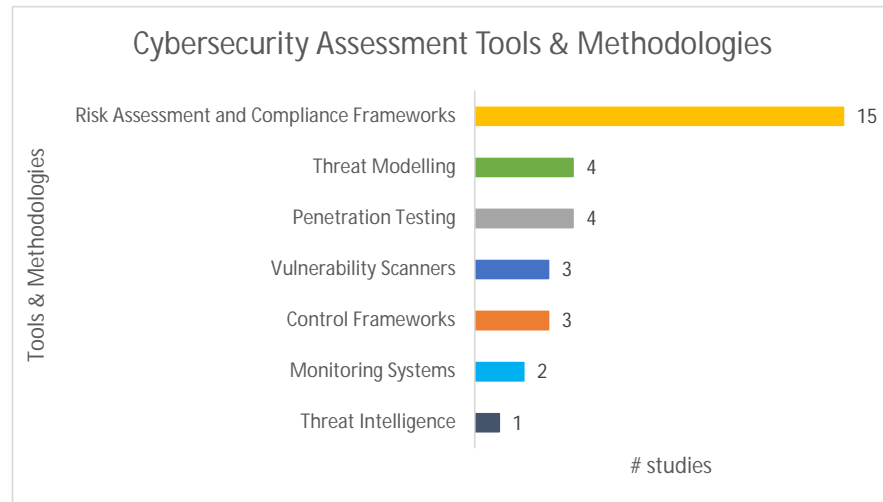
4 papers suggested Threat Modelling methods and tools such as attack trees [26] and Microsoft's STRIDE [7,12,35] while 3 papers suggested using Vulnerability Scanners like OpenVAS and OWASP ZAP [36,37], and Nessus [35]. On the other hand, 3 papers suggested using Control Frameworks like CIS Controls (CIS-Centre for Internet Security) and CSA CCM (Cloud Security Alliance Cloud Controls Matrix) [10], and Zero Trust Model [38,39] while 2 papers recommended using Monitoring Systems like SIEM (Security information and event management), IDS/IPS (Intrusion Detection Systems/Intrusion Prevention Systems), DLP (Data Leakage Prevention), Threat Intelligence [8,39]. There was only 1 primary paper that suggested employing Threat Intelligence [39]. 18 primary papers did not mention or suggest any assessment tools or methodologies. Figure 6 shows the detailed distribution of cybersecurity assessment tools and methodologies among the primary papers.

#### 4.2. RQ2. What Factors Influence the Adoption of Cybersecurity Measures in Digital Transformation, and What Are the CSFs During and After the Implementation of Those Cybersecurity Measures?

Both adoption factors and CSFs are considered here. Adoption factors relate to the pre-integration period of cybersecurity measures, i.e., the decision phase, while CSFs relate to the actual integration, post-integration, and operation phases. Both are related in some regard to the five cybersecurity governance process categories set out in Section 2, highlighting the multifaceted nature of cybersecurity integration in digital transformation. The required synergy between the two phases ensures that cybersecurity measures are not only chosen wisely but also embedded effectively into the organisation's operations, leading to robust and resilient cybersecurity postures. Some factors feature as both adoption



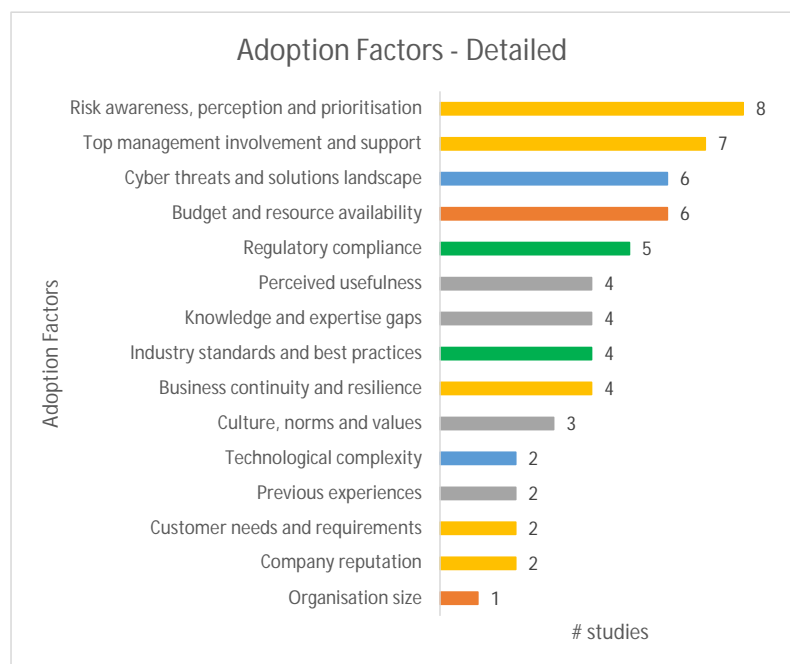
factors and as CSFs. For example, budget and resource availability, encompassed within the Financial process category, is critical not only for adopting cybersecurity measures but also for sustaining and effectively operating the implemented cybersecurity measures. Similarly, top management involvement and support is highlighted in the reviewed papers both as an adoption factor and as an implementation CSF under the process category of Organisational.



**Figure 6.** Detailed distribution of cybersecurity assessment tools and methodologies suggested by primary papers.

#### 4.2.1. Cybersecurity Adoption Factors

From the 34 primary papers reviewed, it was found that 18 discussed or suggested factors that motivate businesses to adopt cybersecurity measures. These were grouped into 15 adoption factors, from the most suggested to the least suggested (Figure 7). Table 6 presents the definitions for each of these adoption factors along with a list of the primary papers supporting each.



**Figure 7.** Detailed distribution of cybersecurity adoption factors.

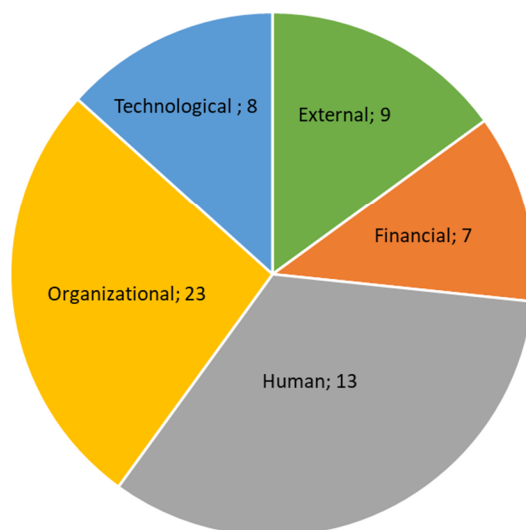
**Table 6.** Definitions of adoption factors, their cybersecurity governance process categories, and supporting primary papers.

Category	Adoption Factor	Definition	Supporting Primary Paper
External	Industry standards and best practices	The established guidelines and procedures widely accepted in the industry for achieving optimal cybersecurity as well as the exemplary actions by other companies	P12, P20, P30, P31
	Regulatory compliance	Adherence to laws, regulations, and standards governing cybersecurity practices have a direct impact on the decisions of companies regarding their cybersecurity measures.	P1, P3, P18, P19, P25
Financial	Budget and resource availability	The financial and material resources allocated for cybersecurity measures, including funding, equipment, and personnel	P3, P9, P21, P23, P30, P32
	Organisation size	The scale of the organisation, often influencing its resource capabilities, complexity of operations, and approach to cybersecurity	P3
Human	Culture, norms, and values	The shared beliefs, practices, and ethical standards (both organisational and national) that influence businesses and their employees' approach to cybersecurity	P8, P10, P30
	Knowledge and expertise gaps	The deficiencies in skills and knowledge within an organisation related to cybersecurity, impacting its ability to protect itself	P8, P21, P30, P31
	Perceived usefulness	The belief in the effectiveness and benefits of cybersecurity measures, influencing their adoption and implementation	P10, P12, P16, P21
	Previous experiences	The historical encounters of an organisation with cyber incidents, shaping its current cybersecurity practices and policies	P20, P30
Organisational	Business continuity and resilience	The ability of an organisation to maintain its essential functions and quickly recover from disruptions caused by cyber incidents	P3, P4, P12, P30
	Company reputation	The public perception and credibility of an organisation, which can be influenced by its cybersecurity practices and incident history. Organisations aiming to protect their cyber reputation tend to prioritise cybersecurity in their business process digitalisation.	P12, P18
	Customer needs and requirements	The expectations and demands of clients and customers regarding the security of their data and interactions with the organisation	P3, P30
	Risk awareness, perception, and prioritisation	This factor is related to how much the organisation is aware of the risks related to their digital business processes, how they perceive risk and accordingly, how they strategically prioritise those risks and their mitigating actions.	P1, P3, P4, P7, P21, P25, P30, P32
	Top management involvement and support	The active participation and backing of an organisation's leadership in cybersecurity initiatives. This factor highlights that cybersecurity is a strategic concern that requires the attention of top management, not just cybersecurity experts.	P1, P4, P8, P10, P18, P23, P25
Technological	Cyber threats and solutions landscape	The current environment of cyber risks, including emerging threats and the range of available technologies and strategies to counter them. The complexity and breadth of threats and solutions can lead to some threats and measures being overlooked.	P1, P7, P8, P16, P30, P31
	Technological complexity	The intricacy of an organisation's IT infrastructure, which can impact the ease and effectiveness of implementing cybersecurity measures	P30, P31

Table 6 also groups the adoption factors by cybersecurity governance process category and the allocation by process category is depicted graphically in Figure 8. The most cited adoption factor was Risk Awareness, Perception, and Prioritisation (8 papers), which falls within the Organisational process category. This factor is related to how much the organisation is aware of the risks related to digitalisation, how they perceive risk and accordingly, how they strategically prioritise those risks and their mitigating actions. For instance, Hidayat and Wang [8] suggested that knowing the impact of data breaches and having examples of other cybersecurity incidents have a clear influence over an organisation's adoption decisions for cybersecurity measures. Similarly, Ghani et al. [35] mentioned the

importance of risk impact awareness, while Chatterjee [40] as well as Wessels et al. [41] highlighted the critical role of risk prioritisation when adopting cybersecurity measures.

### Adoption Factors Cybersecurity Governance Process Categories



**Figure 8.** Distribution of adoption factors by cybersecurity governance process category.

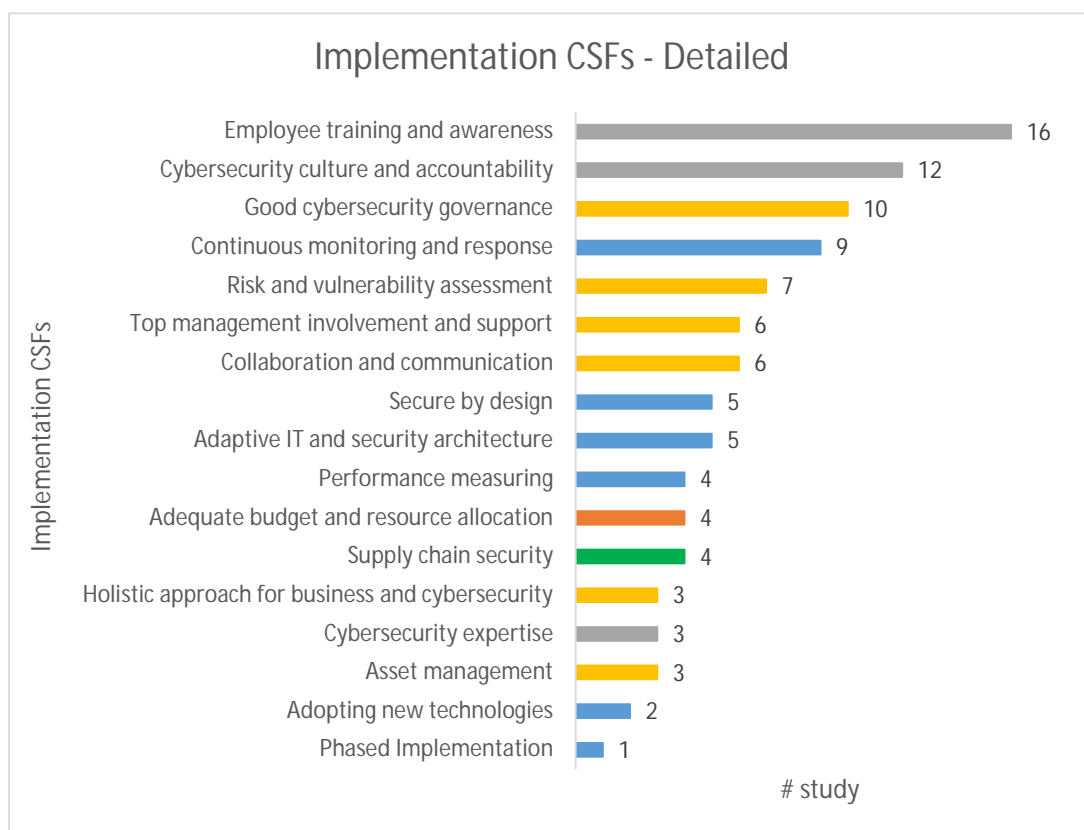
The second most suggested adoption factor was Top Management Involvement and Support, with 7 papers highlighting its significance. For example, Franke and Wernberg [5] (p. 5) stated that “cyber security is a strategic concern, one that cannot be delegated solely to experts, but has to be addressed by top management”. Overall, it is clear from the primary papers that effective management, leadership, and active involvement of top management are crucial for adopting cybersecurity measures. Cyber Threats and Solutions Landscape, with 6 papers, was the next most cited factor. When there are a lot of cyber threats and the solutions landscape is wide and complex, companies find it challenging to identify which threat to focus on, and which measure to prioritise, and some cyber threats and related measures can be overlooked. This factor is actually directly related to the first factor, i.e., risk awareness, perception, and prioritisation. Wessels et al. [41] stated that organisations can be incentivised or de-incentivised due to the existence of competing problems/solutions, i.e., technological complexity. They suggested that “an organisation might not be in the position to invest in all and might have to choose in what to invest given its own priorities: organisations have to assess what issues are most urgent to address” (p. 5).

Budget and Resource Availability, which was cited by 6 primary papers, is related to resources like money, workforce, time, and equipment, and how a lack of these resources can impede taking necessary cybersecurity measures. Other notable adoption factors extracted from the reviewed literature include Regulatory Compliance (5 primary papers) and Industry Standards and Best Practices (4 primary papers), both of which are external factors. Chatterjee [40] mentioned how legislations like the General Data Protection Regulation (GDPR) and the Copyright, Designs and Patents Act 1988 (CDPA) have an imposing effect on companies and their executives to commit to protecting customer data by implementing necessary cybersecurity measures. The author stated that “none of these legislations would be necessary if organisations acted responsibly and proactively on their own. Unfortunately, fear and threats continue to be the most effective motivators for desired corporate behavior” [40] (p. 2). The distribution of the remaining adoption factors is indicated in Figure 7 and their process categorisation is shown in Figure 8. It is evident that these factors complement each other and do not operate in isolation. They form a complex, interdependent network where the strength or weakness of one factor can directly influence

others, sometimes amplifying or diminishing their effects. For instance, if a company has the necessary budget and resources but is not aware of cybersecurity risks, it may fail to take the necessary precautions. Without risk awareness, even well-funded organisations may allocate their resources ineffectively or under-prioritise critical cybersecurity measures. Similarly, an organisation may have a clear understanding of the need for cybersecurity, but if the solutions are perceived as overly complex or incompatible with existing infrastructure, the implementation might stall, even with senior management support. Successful cybersecurity adoption requires coordinated action across all process categories.

#### 4.2.2. Critical Success Factors for Implementing Cybersecurity Measures

Out of the 34 primary papers reviewed, 27 of them discussed CSFs related to the implementation of cybersecurity measures when digitalising business processes. These were grouped into 17 CSFs based on their common characteristics, ranging from the most suggested (employee training and awareness) to the least suggested (phased implementation) (Figure 9). Table 7 presents the definitions for each of these CSFs along with a list of the primary papers supporting them. These CSFs are further grouped into the 5 cybersecurity governance process categories in Figure 10.



**Figure 9.** CSFs for cybersecurity implementation.

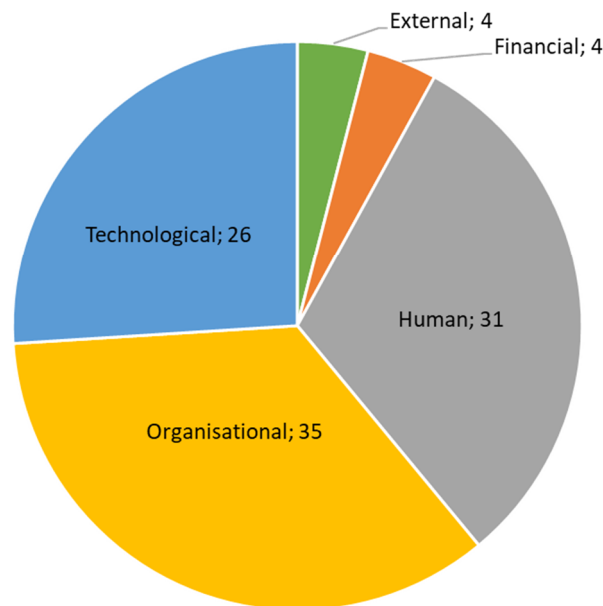
Employee Training and Awareness stands out as the most highlighted CSF and in this context, several papers suggested that humans are the weakest link in cybersecurity [2,7,40]. To quote from Hidayat and Wang [8] (pp. 537–538), “the organisation needs to ensure proliferation of cybersecurity awareness across the organisation as it increasingly innovates and integrates new technologies (e.g., cloud computing) and embrace new ways of working (e.g., agile development). All stakeholders (i.e., board, leaders, management and employees) need to gain an appreciation of the associated cyber threats and risks” [8].

**Table 7.** Definitions of implementation CSFs, their cybersecurity governance process categories, and supporting primary papers.

Category	Implementation CSFs for Cybersecurity Measures	Definition	Supporting Primary Paper
External	Supply chain security	Managing and securing the supply chain to protect against risks associated with third-party vendors and partners.	P1, P3, P8, P24
Financial	Adequate budget and resource allocation	Ensuring sufficient financial and human resources are allocated to cybersecurity initiatives.	P1, P9, P23, P25
Human	Cybersecurity culture and accountability	Building a strong cybersecurity culture where security is prioritised, and everyone is accountable for protecting the organisation's digital assets.	P1, P5, P8, P9, P10, P16, P18, P21, P22, P25, P29, 34
	Cybersecurity expertise	Having skilled and knowledgeable personnel dedicated to cybersecurity.	P5, P23, P31
	Employee training and awareness	Conducting regular training programs and awareness campaigns to educate employees about cybersecurity risks, best practices, and their role in maintaining security.	P1, P5, P7, P8, P9, P10, P12, P14, P18, P21, P22, P25, P27, P29, P31, P34
Organisational	Asset management	Effective management of all organisational assets, including hardware, software, data, and intellectual property.	P1, P2, P33
	Collaboration and communication	Promoting open and effective communication and collaboration across all levels of the organisation.	P1, P5, P6, P7, P31, P34
	Good cybersecurity governance	Establishing a structured framework of policies, procedures, and practices that ensure an organisation's information and systems are secure, resilient, and aligned with business objectives.	P1, P5, P9, P10, P18, P21, P23, P25, P31, P34
	Holistic approach for business and cybersecurity	Integrating cybersecurity into all aspects of business operations and decision-making.	P5, P16, P23
	Risk and vulnerability assessment	Conducting comprehensive assessments to identify, evaluate, and prioritise risks and vulnerabilities in the organisation's IT systems and business processes.	P1, P2, P5, P9, P12, P14, P34
	Top management involvement and support	Securing active involvement and commitment from top management in cybersecurity initiatives.	P5, P10, P18, P23, P25, P34
	Technological	Adaptive IT and security architecture	The ability to design and implement flexible, scalable, and robust IT and security infrastructures that can adapt to evolving threats, technological advancements, and changing business needs.
Adopting new technologies		The proactive adoption and integration of emerging technologies that enhance cybersecurity capabilities.	P1, P31
Continuous monitoring and response		Implementing systems and processes for the ongoing monitoring of networks, systems, and data to detect and respond to security incidents in real time.	P1, P6, P12, P14, P23, P28, P31, P33, P34
Performance measuring		Implementing metrics and key performance indicators (KPIs) to assess the effectiveness of cybersecurity initiatives.	P1, P5, P20, P33
Phased Implementation		Adopting a phased approach to implementing cybersecurity measures, allowing for gradual integration, and testing of new technologies and processes.	P9
Secure by design		Ensuring that security is integrated into the design and development of systems, applications, and processes from the outset.	P1, P8, P13, P26, P29

The second most cited CSF was Cybersecurity Culture and Accountability with 12 out of 34 papers emphasising it. This CSF falls under the Human process category. Cybersecurity is not one person's or one specific team's job [8]. The whole company should take responsibility and assume accountability and joint ownership when it comes to protecting the organisation against cyber risks and threats [40]. This includes employees both at the top floor and on the shop floor. Each employee must do their best to comply with cybersecurity rules and protocols of the company as well as the external standards and regulations.

## Integration CSFs Cybersecurity Governance Process Categories



**Figure 10.** CSFs for cybersecurity implementation by cybersecurity governance process category.

To achieve this, Uchendu et al. [42] suggested using rewards and sanctions to promote cybersecurity culture and accountability among employees. Perera et al. [43] (p. 19) noted that employees should “feel that they are part of the solution”, highlighting the importance of internalising cybersecurity behaviour and culture. Salin [44] (p. 207) discussed establishing “Security Champion teams” which consists of “dedicated individuals from various departments within an organisation, serving as the liaison between their own teams and the security team to bolster cybersecurity measures. These individuals are trained to identify and mitigate security risks, educate colleagues on best practices, and cultivate a security-conscious culture, empowering every employee to take ownership of their role in protecting the organisation’s digital assets”. To quote from Abu Othman et al. [45] (p. 1), “all security countermeasures become worthless if the users do not comprehend the importance of security, do not comply with the policies, and disable or avoid security implementation for personal gain”. This clearly underscores the importance of establishing a companywide cybersecurity culture.

The third most mentioned implementation CSF was Good Cybersecurity Governance, pointed out in 10 papers. Through good cybersecurity governance, a structured framework and a clear cybersecurity roadmap can be established within the organisation to tackle cybersecurity risks and threats. In order for cybersecurity measures to be successful, they must be strategically planned, implemented, and monitored, all of which are part of cybersecurity governance. Having an effective cybersecurity strategy is of utmost importance for the success of cybersecurity measures [46]. Another important aspect of good cybersecurity governance is having robust security policies and protocols [2,42,47,48]. Preparing internal security policies and protocols and making sure that the whole organisation abides by them is integral to cybersecurity governance. Furthermore, governance is related to alignment with risk management and existing frameworks, establishing ownership for assets, and creating risk awareness as specified by Bobbert and Scheerder [42].

Continuous Monitoring and Response was another commonly mentioned CSF, being in 9 primary papers. This CSF has two focuses. The first is monitoring implemented cybersecurity measures to ensure they are effective in protecting the organisation [4,6,38,39,49,50].



The second focus is about being vigilant and up to date regarding potential cyber threats and new attack types [8,48,51].

The distribution of the other CSFs is shown in Figure 9 and their cybersecurity governance process categories are displayed in Figure 10. These CSFs sometimes overlap and complement each other when it comes to implementing cybersecurity measures successfully. For instance, having good cybersecurity expertise within the company but failing to establish a proper cybersecurity culture would hamper the effectiveness of the implemented cybersecurity measures. In similar vein is the connection between adequate budget and resource allocation and good cybersecurity governance. Without sufficient resources, even the best intentions and strategies cannot be fully executed. As stated by Abd Majid and Zainol Ariffin [51] (p. 5), “coordination between humans, processes, and technologies is essential for establishing harmony between skills, systematic processes, and the technologies that is used to create strong cyber defences to protect organisational assets”.

#### *4.3. RQ3. What Industry Standards/Frameworks, and Regulations Are of Significance for Cybersecurity in the Context of Digital Transformation?*

Using standards and/or frameworks is useful for companies to assess their cybersecurity maturity, while regulations provide a backdrop within which companies must operate. Regulations establish the rules and guidelines that companies are required to follow. They influence and shape business operations by setting boundaries, expectations, and requirements that companies must comply with to operate legally and responsibly. Standards and frameworks help companies assess and audit their cybersecurity measures and maturity levels to ensure they are not only aligned with cybersecurity laws and regulations, but also to ensure the security of their systems and the confidentiality, integrity, and availability of their data.

In the primary papers, 26 different standards/frameworks were identified while the number of regulations identified was 6. These surfaced in 17 papers, with 13 papers highlighting standards/regulations and 7 papers discussing regulations. The international standards and industry frameworks highlighted by the primary papers can be seen in Figure 11, and the regulations in Figure 12.

Table 8 presents a list of all the primary papers corresponding to each cybersecurity standard or framework and regulation. Among the 26 cybersecurity-related international standards/frameworks, 8 were part of the NIST Cybersecurity Framework group, such as NIST SP 800-82 or NIST SP 800-115 [34,52]. The 8 individual standards included various ISO/IEC standards like the ISO/IEC 27000 family and ISO/IEC 15408 [53]. COBIT (Control Objectives for Information and Related Technologies), a widely known industry framework was noted by 4 primary papers. In terms of regulations, 6 different regulations were identified in the literature review that were highlighted by 7 primary papers. These were the European GDPR, Network and Information Security (NIS) Directive, EU Cybersecurity Act, the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), and lastly the CDPA, which is the United States version of GDPR.

The NIST Cybersecurity Framework [54] (p. i) “provides guidance to industry, government agencies, and other organisations to manage cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organisation—regardless of its size, sector, or maturity—to better understand, assess, prioritise, and communicate its cybersecurity efforts”. Of the 12 papers referring to this framework, some addressed only one of the NIST publications while some mentioned more than one. These include the NIST Cybersecurity Framework (5 papers), NIST SP 800-53 (3 papers) [55], NIST SP 800-115 (2 papers), NIST SP 800-82 (1 paper), NIST SP 800-55 (1 paper) [56], NIST SP 800-207 (1 paper) [57], NIST SP 800-124 (1 paper) [58], and the NIST SP 800 group of standards (1 paper). Nicoletti and Appolloni [59], for example, suggested that 5PL (fifth-party logistics operators) should consider using the NIST Cybersecurity Framework (NIST CSF) in their security architecture. They noted that the 5 functions of NIST CSF, namely Identify,

Protect, Detect, Respond, and Recover, would support 5PL digital business ecosystems in managing their cybersecurity risks. Abu Othman et al. [45] discussed the use of the NIST SP 800-124 [60] in auditing mobile device security within the context of BYOD (Bring Your Own Device) policies of companies.

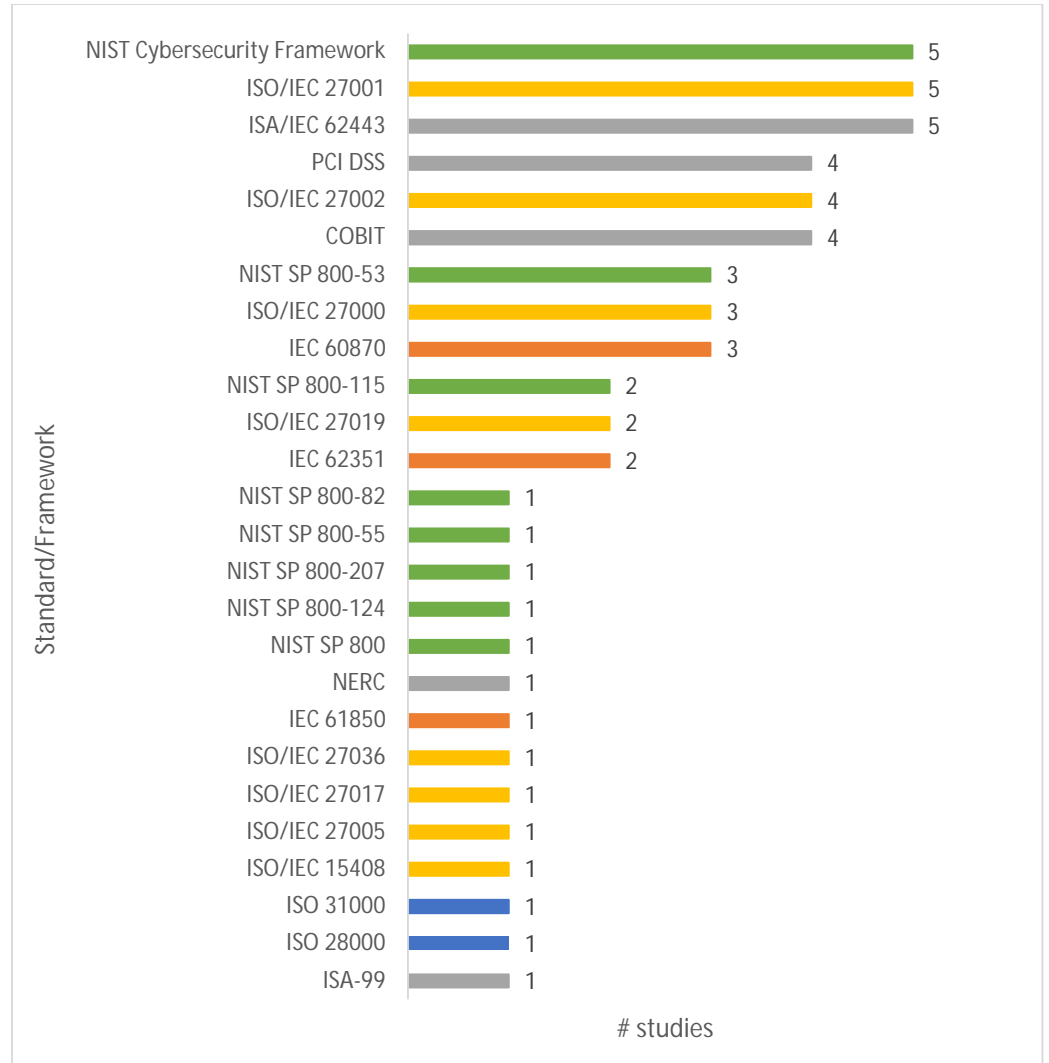


Figure 11. Cybersecurity standards/frameworks noted in the primary papers.

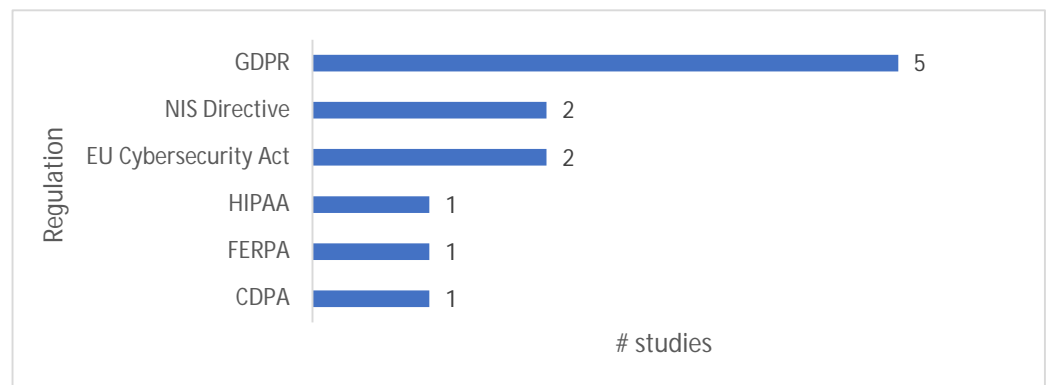


Figure 12. Cybersecurity regulations noted in the primary papers.

**Table 8.** Cybersecurity standards/frameworks and regulations.

<b>Standards/Frameworks</b>	<b>Related Papers</b>
COBIT	P1, P2, P22, P34
IEC 60870	P15, P17, P19
IEC 61850	P15
IEC 62351	P17, P19
ISA/IEC 62443	P9, P15, P17, P19, P20
ISA-99	P9
ISO 28000	P13
ISO 31000	P18
ISO/IEC 15408	P20
ISO/IEC 27000	P3, P22, P34
ISO/IEC 27001	P1, P2, P17, P19, P22
ISO/IEC 27002	P17, P19, P22, P34
ISO/IEC 27005	P15
ISO/IEC 27017	P20
ISO/IEC 27019	P17, P19
ISO/IEC 27036	P15
NERC	P9
NIST Cybersecurity Framework	P1, P9, P12, P13, P22
NIST SP 800	P18
NIST SP 800-115	P17, P19
NIST SP 800-124	P22
NIST SP 800-207	P34
NIST SP 800-53	P2, P19, P20
NIST SP 800-55	P20
NIST SP 800-82	P15
PCI DSS	P1, P17, P19, P34
<b>Regulations</b>	
CDPA	P25
EU Cybersecurity Act	P17, P19
FERPA	P9
GDPR	P9, P10, P12, P14, P25
HIPAA	P9
NIS Directive	P17, P19

Another significant group of standards prevalent among the reviewed primary papers was the ISO/IEC standards, which are the collaborative publications by the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC). In total, 8 different ISO/IEC standards were mentioned by 9 unique primary papers. Some of these papers addressed only one ISO/IEC publication while some mentioned more than one standard. For instance, when discussing cybersecurity assessments in critical infrastructures, specifically energy grid operators, Bartusiak et al. [37] made recommendations about using both ISO/IEC27002 and ISO/IEC 27019 [61,62].

ISA/IEC 62443 was also one of the most mentioned standards with 5 primary papers highlighting it. “The ISA/IEC 62443 series addresses the security of industrial automation and control systems (IACS) throughout their lifecycle. These standards and technical reports were initially developed for the industrial process sector, but have since been applied to building automation, medical devices and transportation sectors” [33] (p. 2). Another important standard mentioned by 4 different primary papers was the PCI DSS (Payment Card Industry Data Security Standard) published by the PCI Security Standards Council. “PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps that mirror security best practices” [63] (p. 9).

COBIT (Control Objectives for Information and Related Technologies) was the next most mentioned framework. “COBIT defines the design factors that should be considered by each enterprise to build a best-fit governance system focusing on the context, objectives and needs of the enterprise” [64] (p. 13). These design factors include processes; organisational structures; information flows and items; people, skills, and competencies; principles, policies, and procedures; culture, ethics, and behaviour; services, infrastructure, and applications.

Of the regulations related to cybersecurity, GDPR was mentioned by 5 papers, the NIS Directive, and the EU Cybersecurity Act, mentioned by 2 papers each, and HIPAA, FERPA, and CDDPA were mentioned by 1 paper each. The GDPR (General Data Protection Regulation) is a data protection law enacted by the EU which the goal of protecting the privacy and personal data of EU citizens. It is “intended to deter misuse and abuse of customer data by companies” [40] (p. 2). The GDPR is a fundamental document in terms of data protection and is therefore integral to cybersecurity, one of the primary goals of which is to protect data. The CDDPA (Consumer Data Protection Act) on the other hand is the USA counterpart of the European GDPR. Similar to the GDPR, CDDPA also aims to safeguard consumer data by regulation how businesses collect, use, and share personal data. The NIS Directive mentioned by [36–39] is an EU directive that aims to enhance the cybersecurity and resilience of critical infrastructure of EU member states by requiring them to implement appropriate security measures. The EU Cybersecurity Act highlighted by 2 primary papers aims to strengthen cybersecurity across the EU by establishing a framework for the certification of information and communications technology (ICT) products, services, and processes. Finally, 2 sector-specific U.S. laws were mentioned by 1 primary paper, i.e., the HIPAA (Health Insurance Portability and Accountability Act), which is a U.S. law that establishes standards to protect the privacy and security of patients’ medical records and other personal health information, and the FERPA (Family Educational Rights and Privacy Act), which protects the privacy of students’ education records. Based on their regions and their sectors, businesses have to abide by these regulations and make sure that their business processes are aligned with the rules stipulated in these cybersecurity related regulations.

#### *4.4. RQ4. What New Cybersecurity Framework Can Be Developed to Coordinate Guidelines, Strategies, and Standards Specifically for SMEs to Complement Current Top-Down Perspectives?*

Cybersecurity is an evolving topic that continuously presents new areas to investigate as technological developments and digitalisation become the norm in both personal and professional lives. Indeed, the studies reviewed here have identified some gaps and limitations in terms of cybersecurity from the perspective of business process digitalisation and made some recommendations for future work in this area. As regards to the cybersecurity adoption factors and implementation CSFs, approximately two-thirds of these factors fall within the Organisational or Human cybersecurity governance process categories, reflecting their overall significance in cybersecurity management.

Other evidence from the cited works underlines the importance of these process categories in cybersecurity. Concerning Organisational factors, a notable gap mentioned by several papers was the lack of clear policies, guidelines, and standards specifically tailored

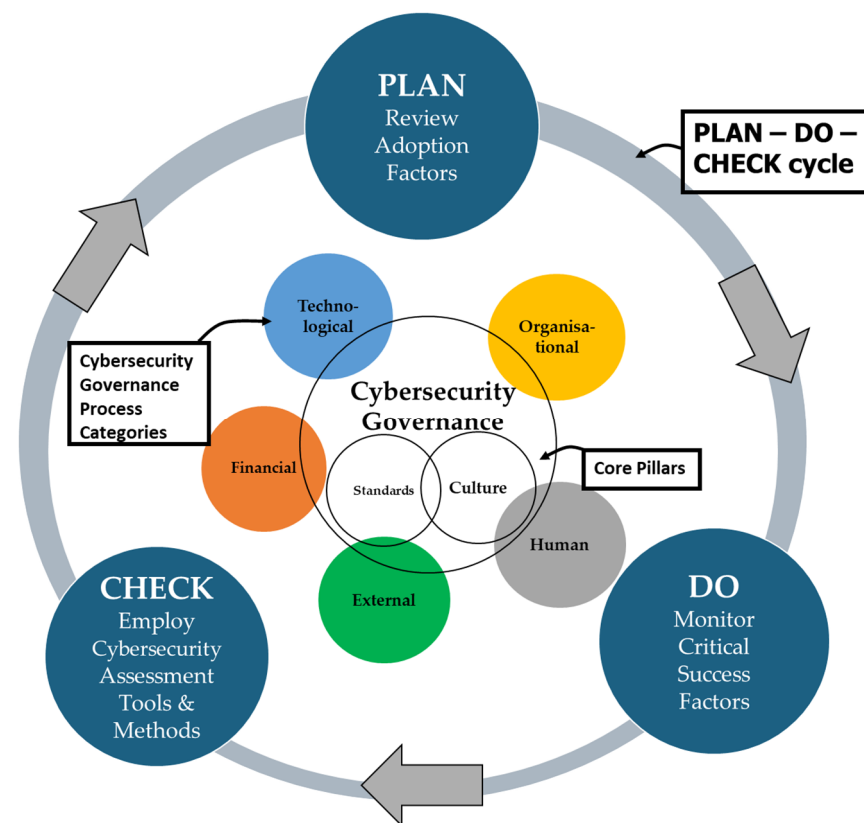
for SMEs to follow, or use on their own [7,11,42]. Uchendu et al. [42] suggested developing and adapting tools and frameworks that are tailored to the needs and resource constraints of SMEs, ensuring they are both affordable and practical for smaller enterprises. Concerning the Human cybersecurity governance process category factors, several papers cited humans as the weakest link in cybersecurity. Many suggested this topic should receive special and continuous attention if businesses want to be successful in their cybersecurity endeavours [4,65,66]. Focusing on Employee Awareness and Training as a CSF for the cybersecurity standing of an organisation, Salamah et al. [65] highlighted the need for customising the training programmes according to the characteristics and needs of the organisation and their employees, and that the prevalent one-size-fits-all approach is a limitation to the success of cybersecurity training efforts for employees. They suggested future work should focus on developing an “adaptive cybersecurity training (ACST) programme” (p. 459) to truly increase the awareness of employees on cybersecurity.

Within the Technological cybersecurity governance process category, a common theme highlighted in the literature was that current methods for identifying security related issues seem to be insufficient with respect to new technologies like IoT, cloud computing, 5G, quantum computing, AI and the metaverse [1,2,4,67–69]. To combat this, the reviewed articles make several suggestions for future work, such as developing new paradigms that emphasise secure application development, creating and implementing intelligent tools that assist in auditing system security [1], prioritising comprehensive risk assessment for emerging technologies and engaging in “futuristic technological forecasting” and cybersecurity planning [4], updating and adapting company’s strategic planning processes to better align with and address new cybersecurity challenges and opportunities [2], and automating the security assessments through advanced natural language processing methods [37].

In Figure 13, an operational framework is put forward for cybersecurity governance based on the SLR and related analysis. The framework resembles Deming Cycle’s Plan-Do-Check-Act (PDCA) model; however, for the sake of simplicity, the Act and Plan steps have been combined: It is a PDC Cycle.

Each phase of the PDC cycle plays a key role in the continuous improvement and management of cybersecurity processes. This framework synthesises the findings from all RQs, aligning them with specific steps of the cycle. RQ2 informs both the PLAN and DO phases, contributing to the identification of adoption factors in the planning stage and addressing CSFs during implementation. Findings from RQ1 support the CHECK phase, focusing on the evaluation of cybersecurity processes through assessment methods and tools. The framework revolves around the cybersecurity governance process categories and their related factors that shape cybersecurity strategy and guide continuous improvement: i.e., the human, external, financial, technological, and organisational process categories.

The related standards and best practices discussed in answer to RQ3 contribute to all three steps of the presented framework. During the PLAN phase, organisations focus on identifying risks, establishing security policies, and developing strategies. Standards such as ISO/IEC 27001 are essential in creating information security management systems and setting policies, while the NIST Cybersecurity Framework is widely used to identify and manage security risks. COBIT assists in defining IT management and governance processes, and ISO 31000 provides a framework for risk management. In the DO phase, the planned measures are implemented to protect the organisation. PCI DSS is particularly useful for implementing security measures around payment card data. NIST SP 800-53 ensures the application of security and privacy controls, and ISA/IEC 62443 focuses on applying security measures to industrial automation and control systems. For the CHECK phase, which involves reviewing and evaluating the effectiveness of the implemented security measures, standards such as ISO/IEC 27002 provide guidance on reviewing security controls. NIST SP 800-115 offers guidance for conducting security assessments and penetration testing, and ISO/IEC 27019 supports control procedures within the energy sector by ensuring the implementation of proper information security practices.



**Figure 13.** Operational framework for cybersecurity governance.

At the heart of the proposed framework stand three core pillars: Cybersecurity Governance, Culture, and Standards/Frameworks/Best Practices, that have their foundation in the cybersecurity governance process categories and affect all three phases of PLAN, DO, and CHECK. A comprehensive cybersecurity framework can be effectively structured around these three pillars. Cybersecurity Governance is an Organisational factor that plays a crucial role in integrating cybersecurity across all business processes by ensuring that security policies, procedures, and financial oversight are aligned with the organisation's strategic goals and regulatory requirements. This governance ensures that cybersecurity is not just an IT concern but is embedded across all business operations, with financial resources allocated to prioritise and sustain cybersecurity initiatives. Culture is equally important in the presented framework, as it focuses on embedding cybersecurity awareness and practices into the daily activities of employees. It is built upon several of the Human cybersecurity governance process category factors and should ensure that all personnel are proactive in identifying and mitigating risks, thus reducing the likelihood of human error compromising business processes. Finally, Standards provide the necessary technical and procedural guidelines that ensure consistent and effective implementation of cybersecurity measures across all business processes. They are related to the External cybersecurity governance process category factors and are crucial for maintaining the integrity, availability, and confidentiality of information, thereby safeguarding the organisation against cyber threats that could disrupt business operations. By integrating these three pillars across all processes, businesses can ensure that cybersecurity supports both operational resilience and strategic objectives.

## 5. Conclusions

This systematic literature review provided a comprehensive analysis of cybersecurity measures within the context of business digitalisation. The authors believe that the proposed operational framework and associated analysis from the extant literature can be



of value as a guide for SMEs, in particular those with limited resources. The presented framework will be useful for digital transformation initiatives, from planning and adopting secure technologies to continuously evaluating and improving security protocols.

One might argue that SMEs can use existing security standards as guidance for cybersecurity. There are two issues here, however. The first issue is that ISO standards are often too general for practical implementation and do not keep pace with emerging technology trends. For instance, ISO/IEC 27001:2013 [70] did not include requirements for data loss prevention solutions, a gap only addressed in ISO/IEC 27001:2022 after nine years [71]. This demonstrates that relying solely on standards is insufficient for adopting new technologies. The second issue is that the standards are intended to be adapted to a wide range of organisations, so highly talented security experts are needed to interpret them. SMEs may not have such highly qualified experts with high salaries. Other enterprises may address this challenge by leveraging consultancy and outsourcing services. This study presents all related standards, best practices, and frameworks for SMEs, based on the reviewed literature as set out in the response to RQ3.

The systematic literature review revealed that effective integration of cybersecurity measures is underpinned by several CSFs. In this regard, employee training and awareness emerged as the most crucial factor from the reviewed primary papers, emphasising the need for continuous education and vigilance to mitigate human-related cybersecurity vulnerabilities [72]. Establishing a strong cybersecurity culture [73] and accountability throughout the organisation, together with continuous monitoring and response capabilities were also found to be essential for ensuring the effectiveness of cybersecurity measures. The review also emphasised the importance of using international standards and industry frameworks, like the NIST Cybersecurity Framework and various ISO/IEC standards, which provide structured approaches for assessing and managing cybersecurity risks, to enhance cybersecurity practices of organisations. These frameworks help organisations align their cybersecurity practices with regulatory requirements and industry best practices, enhancing overall security and compliance.

Senior management in an SME may decide to implement ISO 27001 information security management standards and expect the IT team to follow this decision. This approach is known as a top-down approach. Just as in farming, where understanding the environment is crucial before planting seeds, so too in business, it is vital to assess the conditions before implementing a strategy. A top-down approach for SMEs may look like planting seeds and expecting a harvest without first examining the soil, seasons, and climate conditions. As opposed to current top-down approaches that are more applicable for larger organisations, this framework makes use of a bottom-up approach which is suitable for SMEs, and which is focused on coordinating guidelines, strategies, and standards, and is therefore believed to be more beneficial for SMEs, who often will not have the resources to adopt top-down approaches.

This article clearly has its limitations. The operational framework is based on concepts derived from the extant literature and developed through subsequent analysis and synthesis of previous works. The framework thus remains in the main theoretical, and has not been deployed in real-life case studies or received practitioner review and validation. It should thus best be viewed as a prototype that requires testing and application in real-world business environments. Nevertheless, the operational framework is rooted in the principles of the PDCA cycle, offering a comprehensive and systematic approach to embedding cybersecurity within company digitalisation. The three iterative phases of planning, implementation, and evaluation (plan-do-check) can engender continuous improvement in managing cybersecurity risks. The integration of core pillars and cybersecurity governance process categories underscores the framework's emphasis on creating a resilient organisational environment where cybersecurity is not merely a technical concern, but a strategic imperative deeply ingrained into everyday business operations. The framework can serve as a robust foundation for organisations seeking to protect their assets, ensure compliance, and maintain competitive advantage in an increasingly digitalised business landscape.

As noted above, future research could progress the development of the operational framework through practitioner feedback and application in the SME environment, and other studies could address related areas identified in the SLR. The lack of clear policies, guidelines, and standards specifically tailored for addressing the needs of SMEs warrants further attention, as does the need to develop customised standards for emerging technologies like IoT and AI. Another gap identified through the reviewed primary papers was the need for developing custom training programs to adapt to the characteristics of different organisations, employees, and job roles. Furthermore, while the framework provides a robust structure for addressing cybersecurity challenges in digitalisation, future research could examine how this framework relates to existing cyber maturity models, such as the CMMI Cyber Maturity Platform [74] and the Sectoral Cybersecurity Maturity Model by the World Bank Group [75]. One point of difference is that the framework developed here addresses aspects such as organisational culture and governance in a more integrated and practical manner than other frameworks. The empirical validation of the framework could involve field testing in SMEs across various industries. This would provide practical insights that could help refine the framework and adapt it more effectively to the specific needs and contexts of different organisations.

Overall, this study provides valuable insights for both researchers and practitioners, offering a strategic roadmap for integrating robust cybersecurity measures into business digitalisation initiatives. By addressing the identified gaps and utilising the adoption factors and CSFs, organisations can enhance their cybersecurity posture and ensure the resilience and continuity of their business operations. Such initiatives will contribute to a more secure digital transformation, safeguarding sensitive information, maintaining operational integrity, and building trust with customers and stakeholders.

**Author Contributions:** Conceptualization, F.G.Ö., B.M. and M.W.; methodology, F.G.Ö.; validation, B.M., F.G.Ö. and M.W.; formal analysis, F.G.Ö.; investigation, F.G.Ö.; resources, F.G.Ö.; data curation, F.G.Ö.; writing—original draft preparation, F.G.Ö.; writing—review and editing, F.G.Ö., B.M. and M.W.; visualization, F.G.Ö., B.M. and M.W.; supervision, B.M.; project administration, B.M., F.G.Ö. and M.W. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** The original contributions presented in the study are included in the article and appendices. Further inquiries can be directed to the corresponding author.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## Appendix A

Table A1. Full list of primary papers.

ID	Ref #	Related RQs	Title	Author/Year	Objective	Research Strategy	Methodology	Data Collection Methods	Subjects	Country/Region	Online Database/Publisher	Document Type	Cybersecurity Theme
P1	[8]	RQ1 RQ2 RQ3	A Comprehensive Cybersecurity Maturity Study for Nonbank Financial Institution	Hidayat & Wang (2023)	The goal of the article is to assess the operational effectiveness of implemented cybersecurity measures at an Indonesian Life Insurance company using the NIST Cybersecurity Framework version 1.1 to enhance its information security posture and combat cyber threats to support its digitalisation efforts.	Single case study	Mixed methods	Interviews, documentation review, literature review, case study analysis	Staff and stakeholders at an Indonesian Life Insurance firm	Indonesia	Success Culture Press	Article	Cybersecurity assessment
P2	[10]	RQ1 RQ2 RQ3	A modular framework for auditing IoT devices and networks	Rizvi et al. (2023)	This paper aims to present a modular IoT auditing framework tailored for enterprise networks with IoT devices and focuses on strengthening IoT auditing process on a business, technical and operational level.	Conceptual study with case study	Mixed methods	Literature review, case studies, interviews, documentation	19 participants consisting of IT auditors (15 men, 4 women; education ranging from bachelor's to doctoral degree)	x	Elsevier Ltd.	Article	Cybersecurity auditing
P3	[11]	RQ2 RQ3	A Study of Distinguishing Factors between SME Adopters versus Non-Adopters of Cybersecurity Standard	Auyporn et al. (2023)	The study aims to identify factors that differentiate SME adopters from non-adopters of cybersecurity standards in Thailand and to provide recommendations for policymakers to enhance the adoption of these standards among SMEs.	Survey	Quantitative	Online questionnaires	312 SMEs in Thailand. Respondents include SME IT leaders, CTOs, or CEOs	Thailand	University of Bahrain	Article	Cybersecurity adoption/implementation
P4	[5]	RQ2	A survey of cyber security in the Swedish manufacturing industry	Franke & Wernberg (2020)	The goal of the article is to explore cybersecurity practices in Swedish manufacturing companies within the context of Industry 4.0, by mapping risk perception and controls through a sector-wide survey and identifying gaps between digitalisation impacts and cybersecurity measures.	Survey	Quantitative	Online questionnaire	649 respondents from the Swedish manufacturing industry. Respondents include owners, CEOs, C-suite executives, heads of IT	Sweden	Institute of Electrical and Electronics Engineers Inc.	Conference paper	Cybersecurity adoption/implementation
P5	[2]	RQ2	A systematic synthesis of critical success factors for cybersecurity	Yeoh et al. (2022)	The goal of the article is to analyse and synthesize existing studies on cybersecurity critical success factors (CSFs) and to present an overarching CSF framework based on IT capability theory for organisations to use to guide their cybersecurity management.	Systematic literature review	Mixed methods	Literature review	Analysis of 31 research articles	x	Elsevier Ltd.	Article	Cybersecurity management
P6	[6]	RQ2	Agriculture 4.0 and beyond: Evaluating cyber threat intelligence sources and techniques in smart farming ecosystems	Bui et al. (2024)	This paper aims to assess the applicability of existing cyber threat intelligence (CTI) techniques in smart farming infrastructures and to highlight the potential significance of implementing a virtual Chief Information Security Officer (vCISO) to enhance cybersecurity in the agricultural sector.	Systematic literature review	Mixed methods	Literature review	Analysis of 124 selected papers	x	Elsevier Ltd.	Review	Cybersecurity management
P7	Not ref'd directly	RQ2	Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector	Bolat & Kayışoğlu (2019)	This article aims to understand the factors influencing cybersecurity awareness in the Turkish maritime sector, using questionnaire data from maritime employees.	Single case study	Mixed methods	Questionnaire survey, literature review	211 maritime employees in Turkey. Majority (89%) male, various ages, and experience levels	Turkey	TMMOB Chamber of Ship Machinery Management Engineers	Article	Cybersecurity adoption/implementation
P8	[7]	RQ1 RQ2 RQ3	Cybersecurity 4.0: safeguarding trust and production in the digital food industry era	Alqudhaibi et al. (2024)	The goal of the article is to assess the current state of cybersecurity in the food industry and propose a specialized security framework to mitigate risks and enhance cybersecurity preparedness and awareness.	Systematic literature review	Mixed methods	Systematic literature review, online survey	IT employees in the food industry	United Kingdom	Springer Nature	Article	Cybersecurity adoption/implementation
P9	[46]	RQ1 RQ2 RQ3	Cybersecurity in a Large-Scale Research Facility—One Institution's Approach	Butcher et al. (2023)	This article aims to present a cybersecurity approach for the National High Magnetic Field Laboratory at Florida State University, focusing on risk identification and management while balancing the complex needs of research and security.	Single case study	Mixed methods	Documentation review, interviews, literature review, case study analysis	Staff and stakeholders at the National High Magnetic Field Laboratory (NHMFL)	United States	MDPI	Article	Cybersecurity management

Table A1. Cont.

ID	Ref #	Related RQs	Title	Author/Year	Objective	Research Strategy	Methodology	Data Collection Methods	Subjects	Country/Region	Online Database/Publisher	Document Type	Cybersecurity Theme
P10	[42]	RQ2 RQ3	Developing a cyber security culture: Current practices and future needs	Uchendu et al. (2021)	The goal of this article is to conduct a study on organisational cybersecurity culture by investigating its definition, essential factors, proposed frameworks to cultivate cybersecurity culture, and assessment metrics, to provide guidance for both practitioners and researchers.	Systematic literature review	Mixed methods	Systematic literature review	Analysis of 58 research articles	x	Elsevier Ltd.	Article	Cybersecurity management
P11	[12]	RQ1	DigiShip—Digitalisation of ship operations	Yue et al. (2022)	This paper discusses the potential benefits of maritime digitalisation with a focus on remote monitoring and control of machineries and sensors, using threat modelling and risk assessment methodologies, to enhance predictive maintenance and reduce life-cycle costs.	Single case study	Mixed methods	Documentation review, case study analysis	x	Singapore	Institute of Physics	Conference paper	Cybersecurity assessment
P12	[4]	RQ1 RQ2 RQ3	Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations	Saeed et al. (2023)	The goal of the article is to understand the cybersecurity implications of digital transformation for business resilience and to propose a staged cybersecurity readiness framework to help organisations mitigate digital transformation related cybersecurity risks.	Systematic literature review	Mixed methods	Systematic literature review	Review of 42 papers	x	MDPI	Review	Cybersecurity assessment
P13	[59]	RQ1 RQ2 RQ3	Digital transformation in ecosystems: integrated operations model and its application to fifth-party logistics operators	Nicoletti & Appolloni (2024)	The main objective of this article is to present an integrated digital transformation framework for quintile logistics (5PL) companies, focusing on transforming their operating model and applying advanced solutions to enhance collaboration, innovation, and efficiency within the logistics ecosystem.	Conceptual study	Qualitative	Literature review, in-depth interviews	Experts from academia, information and communication technology organisations, and key players in the logistics industry	x	Emerald Publishing	Article	Cybersecurity assessment
P14	[49]	RQ2 RQ3	Digital Transformation of Microgrids: A Review of Design, Operation, Optimization, and Cybersecurity	Irmak et al. (2023)	The goal of the article is to provide a comprehensive review of the future digitalisation of microgrids, discussing the key digital technologies and cybersecurity measures needed to enhance their efficiency, reliability, and resilience, while also addressing the associated barriers and challenges.	Literature review	Qualitative	Literature review	x	x	MDPI	Review	Cybersecurity management
P15	[31]	RQ1 RQ3	Enhancing Resilience in Interconnected Cyber-Physical Power Networks	Chobanov (2023)	The article explores opportunities to improve the security and reliability of expanding electricity networks by integrating information and communication technologies and renewable energy sources.	Literature review	Qualitative	Literature review	x	x	Institute of Electrical and Electronics Engineers Inc.	Conference paper	Cybersecurity management
P16	[66]	RQ2	Evaluating Staff Attitudes, Intentions, and Behaviors Related to Cyber Security in Large Australian Health Care Environments: Mixed Methods Study	Dart & Ahmed (2023)	The goal of the article is to analyse the motivations and behaviours influencing healthcare staff's acceptance and application of cybersecurity measures, and to make recommendations for improving cybersecurity governance in healthcare environments.	Exploratory sequential mixed methods	Mixed methods	Online survey, in-depth interviews	103 health care staff members participated in the survey; 9 staff members participated in interviews	Australia	JMIR Publications Inc.	Article	Cybersecurity management
P17	[36]	RQ1 RQ3	Extended Gap Analysis: An Approach for Security Assessment of Critical Infrastructures	Bartusiak et al. (2022)	The article aims to describe a practical approach for conducting cybersecurity assessments in critical infrastructures through an extended gap analysis, aimed at identifying and addressing discrepancies between existing security measures and regulatory recommendations, with a specific application to a digital substation of a German energy grid operator.	Single case study	Mixed methods	Literature review, case study analysis, documentation review	x	Germany	Institute of Electrical and Electronics Engineers Inc.	Conference paper	Cybersecurity assessment
P18	[43]	RQ1 RQ2 RQ3	Factors Affecting Reputational Damage to Organisations Due to Cyberattacks	Perera et al. (2022)	The goal of the article is to identify key factors determining reputational damage to public and private institutions due to cyberattacks, using the STAR model and expert analysis, to help organisations better manage cyber reputation risks.	Delphi study with literature review	Mixed methods	Literature review, semi-structured and structured interviews	Six experts from both public and private sector organisations in Australia; all holding senior positions	x	MDPI	Article	Cybersecurity management

Table A1. Cont.

ID	Ref #	Related RQs	Title	Author/Year	Objective	Research Strategy	Methodology	Data Collection Methods	Subjects	Country/Region	Online Database/Publisher	Document Type	Cybersecurity Theme
P19	[37]	RQ1 RQ2 RQ3	First step into automation of security assessment of critical infrastructures	Bartusiak et al. (2023)	The goal of the article is to develop and describe a practical approach for conducting cybersecurity assessments in critical infrastructures, specifically through an extended gap analysis, and to present a possible automation strategy for initial security assessments, with a case study on a digital substation of a German energy grid operator.	Conceptual study with case study	Mixed methods	Literature review, documentation review, case study analysis	x	Germany	Elsevier Ltd.	Article	Cybersecurity assessment
P20	Not ref'd directly	RQ1 RQ2 RQ3	Information Security Assessment and Certification within Supply Chains	Santos et al. (2021)	The article proposes a metrics framework for supply chains and organisations in an industrial context, highlighting continuous safety assessment for managing information security.	Conceptual study	Mixed methods	Literature review	x	x	Association for Computing Machinery	Conference paper	Cybersecurity assessment
P21	[47]	RQ2	Information Security at Higher Education Institutions: A Systematic Literature Review	Imbaquingo-Esparza et al. (2022)	The goal of the article is to identify and analyse security issues and measures in Higher Education Institutions related to information protection, particularly in the context of digital transformation	Systematic literature review	Mixed Methods	Systematic literature review	Review of 47 papers	x	Springer Science and Business Media Deutschland GmbH	Conference paper	Cybersecurity management
P22	[45]	RQ1 RQ2 RQ3	Information System Audit for Mobile Device Security Assessment	Abu Othman et al. (2021)	The goal of the article is to explore the feasibility of Information Systems audit in assessing mobile device security, focusing on the risks, vulnerabilities, and perceptions of IS management regarding mobile device security in a Bring Your Own Device (BYOD) setting.	Literature review	Mixed methods	Literature review	x	Malaysia	Institute of Electrical and Electronics Engineers Inc.	Conference paper	Cybersecurity auditing
P23	[51]	RQ2	Model for successful development and implementation of Cyber Security Operations Centre (SOC)	Abd Majid & Zainol Ariffin (2021)	The article aims to identify significant factors contributing to the successful development and implementation of Cyber Security Operations Centres (SOC), and to design a model for SOCs, focusing on human, process, and technology factors, with findings based on a quantitative study.	Quantitative study	Quantitative	Questionnaire survey, literature review	63 respondents from 25 ministries and agencies in Malaysia	Malaysia	Public Library of Science	Article	Cybersecurity management
P24	[67]	RQ2	Securing integration of cloud services in cross-domain distributed environments	Suzic (2016)	The article aims to analyse existing cross-domain service composition approaches for cloud integration platforms, focusing on the security of OAuth 2.0 and UMA protocols, and to present a new tool enabling UMA support in the Apache Camel integration framework, culminating in a security assessment based on the RMIAS framework.	Conceptual study with experimental implementation	Mixed methods	Literature review, experimental implementation	x	x	Association for Computing Machinery	Conference paper	Cybersecurity assessment
P25	[40]	RQ2 RQ3	Should executives go to jail over cybersecurity breaches?	Chatterjee (2019)	The goal of the article is to highlight the importance of senior management's active involvement and commitment in achieving high levels of cybersecurity preparedness and emphasizing the need for a strong cybersecurity governance structure and culture.	Conceptual study	Qualitative	Literature review, expert commentary	x	United States	Taylor and Francis Inc.	Article	Cybersecurity management
P26	[1]	RQ2	Some issues in the Re-engineering of business processes and models by using intelligent security tools	Atymtayeva et al. (2017)	The goal of the article is to analyse the relationship between digitally reengineering business processes and cybersecurity by focusing on secure software application and portal development and using intelligent tools in business process reengineering and proposes a new paradigm for secure application development and communication among stakeholders.	Conceptual study	Mixed methods	Literature review	x	x	SciTePress	Conference paper	Cybersecurity management
P27	[65]	RQ2	The Importance of the Job Role in Social Media Cybersecurity Training	Salamah et al. (2022)	The article aims to investigate the feasibility of an adaptive cybersecurity training system for social media users, identifying key factors such as job role, gender, age, education level, and training preferences, and concluding that job role is the most significant factor for developing an effective training strategy.	Survey with qualitative interviews	Mixed methods	Online survey, semi-structured interviews, literature review	641 Kuwaiti employees in a variety of sectors	Kuwait	Institute of Electrical and Electronics Engineers Inc.	Conference paper	Cybersecurity management

Table A1. Cont.

ID	Ref #	Related RQs	Title	Author/Year	Objective	Research Strategy	Methodology	Data Collection Methods	Subjects	Country/Region	Online Database/Publisher	Document Type	Cybersecurity Theme
P28	[38]	RQ1 RQ2	The risk assessment on the security of industrial internet infrastructure under intelligent convergence with the case of G.E.'s intellectual transformation	Zhao & Wu (2022)	The goal of the article is to study the infrastructure and security features of the industrial internet, propose an infrastructure mode and security evaluation system, and to analyse G.E.'s digital transformation in the industrial internet, and describe industrial internet security research from multiple perspectives.	Single Case Study	Mixed Methods	Literature review, case study analysis	x	China	American Institute of Mathematical Sciences	Article	Cybersecurity assessment
P29	[44]	RQ2	Thrifty Guardians: Overcoming the Challenges of Establishing Security Champions on a Limited Budget	Salin (2023)	This article aims to explore the challenges and strategies for establishing and sustaining a cost-efficient Security Champions team in a mid-size software engineering organisation on a limited budget, identifying key success factors and challenges to enhance security awareness, competence, and focus.	Single case study	Mixed methods	Semi-structured interviews, online self-assessment survey, literature review	11 Security Champion team members & 2 key stakeholders from a midsize software engineering org. in the Nordics. Participants include developers, architects, project managers, system technicians, and security engineers	Nordic countries	Institute of Electrical and Electronics Engineers Inc.	Conference paper	Cybersecurity management
P30	[41]	RQ2	Understanding incentives for cybersecurity investments: Development and application of a typology	Wessels et al. (2021)	The article aims develop a typology of incentives for investing in and managing cybersecurity, providing clarity for scholars and professionals to understand and enhance the adoption of cybersecurity measures in organisations.	Literature review with case study	Mixed methods	Literature review, semi-structured in-depth interviews	10 IT security employees representing 9 organisations	x	Elsevier B.V.	Article	Cybersecurity adoption/implementation
P31	[48]	RQ2	Unlocking the potential of cybersecurity behavior in the metaverse: Overview, opportunities, challenges, and future research agendas	Al-Emran & Deveci (2024)	The goal of the article is to provide an overview of cybersecurity behaviour in the metaverse, identify potential opportunities and challenges, and propose large-scale research agendas to address various aspects such as security, human behaviour, virtual identity management, privacy, legal, ethical issues, and cybersecurity education.	Literature review and interpretive paradigm	Qualitative	Literature review, expert commentary	x	x	Elsevier Ltd.	Article	Cybersecurity management
P32	[35]	RQ1 RQ2	User-centric security assessment of software configurations: A case study	Ghani et al. (2014)	The article aims to propose a user-centric methodology for quantitatively assessing the security of software configurations based on expected economic impact and ranking configurations by security, demonstrated through a case study on Amazon EC2 services.	Single Case Study	Mixed Methods	Documentation review, surveys, case study analysis	x	x	Springer Verlag	Conference paper	Cybersecurity assessment
P33	[50]	RQ2	Zero trust cybersecurity: Critical success factors and A maturity assessment framework	Yeoh et al. (2023)	The goal of the article is to investigate the critical success factors (CSFs) for implementing zero trust cybersecurity and to develop a multi-dimensional CSFs framework and maturity assessment framework to guide organisations in planning, assessing, and managing their zero trust cybersecurity initiatives.	Delphi study	Mixed methods	Semi-structured interviews, literature review,	12 CISO or equivalent level cybersecurity experts from seven sectors in Australia	Australia	Elsevier Ltd.	Article	Cybersecurity adoption/implementation
P34	[39]	RQ1 RQ2 RQ3	Zero Trust Validation: from Practice to Theory: An empirical research project to improve Zero Trust implementations	Bobbert & Scheerder (2022)	The goal of the article is to describe the current state of Zero Trust cybersecurity, identify limitations of existing approaches, propose a framework and associated technology based on critical success factors to align cybersecurity with organisational goals, and validate the framework through empirical research to enhance acceptance and implementation of Zero Trust strategies.	Design Science Research with empirical validation	Mixed methods	Empirical validation with practitioner-oriented research	x	x	Institute of Electrical and Electronics Engineers Inc.	Conference paper	Cybersecurity management



## Appendix B

**Table A2.** Scopus search results for each string.

	Search String	No Exclusion	Year Range Limited to = 2013–2024	+ Language Limited to = {English}	+ Document Type Limited to = {Conference Paper + Article + Book Chapter + Review + Book}
String 1	("cybersecurity" OR "cyber security") AND ("critical success factors" OR "success factors" OR "significant factors" OR "influential factors")	105	101	101	96
String 2	("business processes" OR "digital transformation" OR "digitalization") AND ("security evaluation" OR "security auditing" OR "security assessment")	67	47	44	43
String 3	("business processes" OR "digital transformation" OR "digitalization") AND ("adoption" OR "adopting" OR "implementation" OR "implementing") AND ("cybersecurity measures" OR "cyber security measures")	12	12	12	12

## Appendix C

**Table A3.** Full names of the conferences and journals of primary papers.

ID	Conference & Journal Names
P21	10th Ecuadorian Congress of Information and Communication Technologies (TICEC 2022)
P20	16th International Conference on Availability, Reliability and Security (ARES 2021)
P4	2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA 2020)
P34	29th IEEE Annual Software Technology Conference (STC 2022)
P24	31st Annual ACM Symposium on Applied Computing (SAC 2016)
P22	3rd International Cyber Resilience Conference (CRC 2021)
P29	49th Euromicro Conference on Software Engineering and Advanced Applications (SEAA 2023)
P17	5th International Conference on Smart Energy Systems and Technologies (SEST 2022)
P32	6th International Symposium on Engineering Secure Software and Systems (ESSoS 2014)
P27	7th IEEE European Symposium on Security and Privacy Workshops (Euro S and PW 2022)
P26	7th International Symposium on Business Modeling and Software Design (BMSD 2017)
P15	7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT 2023)
P2, P5, P6, P10, P33	Computers and Security
P30	Digital Business
P8	Discover Food
P14	Energies
P18	Informatics
P3	International Journal of Computing and Digital Systems
P11	International Maritime and Port Technology and Development Conference (MTEC 2022) 4th International Conference on Maritime Autonomous Surface Ships (ICMASS 2022)
P16	JMIR Human Factors
P9	Journal of Cybersecurity and Privacy
P7	Journal of Eta Maritime Science
P13	Journal of Global Operations and Strategic Sourcing
P25	Journal of Organizational Computing and Electronic Commerce
P1	Journal of System and Management Sciences
P28	Mathematical Biosciences and Engineering
P23	PLoS ONE
P12	Sensors
P19	Sustainable Energy, Grids and Networks
P31	Technology in Society

## References

1. Atymtayeva, L.; Tulemissova, G.; Nurmyshev, S.; Kungaliyev, A. Some issues in the Re-engineering of business processes and models by using intelligent security tools. In *Proceedings of the 7th International Symposium on Business Modeling and Software Design—BMSD 2017*; SciTePress: Lisbon, Portugal, 2017; pp. 199–205. [CrossRef]
2. Yeoh, W.; Wang, S.; Popovič, A.; Chowdhury, N.H. A systematic synthesis of critical success factors for cybersecurity. *Comput. Secur.* **2022**, *118*, 102724. [CrossRef]
3. Schatz, D.; Bashroush, R.; Wall, J. Towards a More Representative Definition of Cyber Security. *J. Digit. Forensics Secur. Law* **2017**, *12*, 8. [CrossRef]
4. Saeed, S.; Altamimi, S.A.; Alkayyal, N.A.; Alshehri, E.; Alabbad, D.A. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors* **2023**, *23*, 6666. [CrossRef]
5. Franke, U.; Wernberg, J. A survey of cyber security in the Swedish manufacturing industry. In *Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA, Dublin, Ireland, 15–19 June 2020*; p. 9139673.
6. Bui, H.T.; Aboutorab, H.; Mahboubi, A.; Gao, Y.; Sultan, N.H.; Chauhan, A.; Parvez, M.; Bewong, M.; Islam, R.; Islam, Z.; et al. Agriculture 4.0 and beyond: Evaluating cyber threat intelligence sources and techniques in smart farming ecosystems. *Comput. Secur.* **2024**, *140*, 103754. [CrossRef]
7. Alqudhaibi, A.; Krishna, A.; Jagtap, S.; Williams, N.; Afy-Shararah, M.; Salonitis, K. Cybersecurity 4.0: Safeguarding trust and production in the digital food industry era. *Discov. Food* **2024**, *4*, 2. [CrossRef]
8. Hidayat, V.K.; Wang, G. A Comprehensive Cybersecurity Maturity Study for Nonbank Financial Institution. *J. Syst. Manag. Sci.* **2023**, *13*, 525–543.
9. Wynn, M.; Felser, K. Digitalisation and Change in the Management of IT. *Computers* **2023**, *12*, 251. [CrossRef]
10. Rizvi, S.; Zwerling, T.; Thompson, B.; Faiola, S.; Campbell, S.; Fisanick, S.; Hutnick, C. A modular framework for auditing IoT devices and networks. *Comput. Secur.* **2023**, *132*, 103327. [CrossRef]
11. Auyporn, W.; Piromsopa, K.; Chaiyawat, T. A Study of Distinguishing Factors between SME Adopters versus Non-Adopters of Cybersecurity Standard. *Int. J. Comput. Digit. Syst.* **2023**, *13*, 671–680. [CrossRef]
12. Yue, S.P.; Chua, T.Y.; Fan, J.W. DigiShip—Digitalisation of ship operations. *J. Phys. Conf. Ser.* **2022**, *2311*, 012001. [CrossRef]
13. Obwegeser, N.; Yokoi, T.; Wade, M.; Voskes, T. 7 Key Principles to Govern Digital Initiatives—Research and Survey Data Provide Insights for How Leaders Can Govern Digital Initiatives for Maximum Impact. MIT Sloan Management Review—Frontiers—Research Highlight 2020. Available online: <https://sloanreview.mit.edu/article/7-key-principles-to-govern-digital-initiatives/> (accessed on 4 April 2024).
14. Remenyi, D.; Williams, B.; Money, A.; Swartz, E. *Doing Research in Business and Management, an Introduction to Process and Method*; Sage Publications: London, UK, 1998.
15. Akeel, H.; Wynn, M. ERP Implementation in a Developing World Context: A Case Study of the Waha Oil Company, Libya. In *Proceedings of the 7th International Conference on Information, Process and Knowledge Management, Lisbon, Portugal, 22–27 February 2015*; pp. 126–131. Available online: <https://eprints.glos.ac.uk/2072/> (accessed on 10 September 2024).
16. Wynn, M.; Olubanjo, O. Demand-supply chain management: Systems implications in an SME packaging business in the UK. *Int. J. Manuf. Res.* **2012**, *7*, 198–212. [CrossRef]
17. Bakeer, A.; Wynn, M. ICT Utilization in Libyan Universities: A Report on Case Study Research. In *Proceedings of the Ninth International Multi-Conference on Computing in the Global Information Technology, Seville, Spain, 22–24 June 2014*; Think-Mind/ICCGI 2014. pp. 165–170. Available online: <https://eprints.glos.ac.uk/2081/> (accessed on 29 September 2024).
18. Senkus, P.; Glabiszewski, W.; Wysokińska-Senkus, A.; Pańka, A. Process Definitions—Critical Literature Review. *Eur. Res. Stud. J.* **2021**, *24*, 241–255. [CrossRef]
19. Bechara, F.R.; Schuch, S.B. Cybersecurity and global regulatory challenges. *J. Financ. Crime* **2021**, *28*, 359–374. [CrossRef]
20. NordLayer. Cost-Benefit Analysis of Cybersecurity Spending. 2023. Available online: <https://nordlayer.com/blog/cost-benefit-analysis-of-cybersecurity-spending/> (accessed on 6 September 2024).
21. Ogono, U. What Cyber Security Processes Does a Cyber Security Analyst Need to Know? Career Karma, 4 September 2022. Available online: <https://careerkarma.com/blog/cyber-security-processes-and-methods/#:~:text=What%20Is%20a%20Cyber%20Security,and%20defend%20against%20cyber%20crime> (accessed on 2 October 2024).
22. Miles, M.B.; Huberman, M. *Qualitative Data Analysis: An Expanded Sourcebook*, 2nd ed.; Sage Publications, Inc.: Thousand Oaks, CA, USA, 1994; ISBN 9781506353081.
23. Loaiza, J.H.; Cloutier, R.J.; Lippert, K. Proposing a Small-Scale Digital Twin Implementation Framework for Manufacturing from a Systems Perspective. *Systems* **2023**, *11*, 41. [CrossRef]
24. Kitchenham, B.; Charters, S. Guidelines for Performing Systematic Literature Reviews in Software engineering (Technical Report EBSE 2007-001). Keele University and Durham University Joint Report. 2007. Available online: [https://legacyfiles.elsevier.com/promis\\_misc/525444systematicreviewguide.pdf](https://legacyfiles.elsevier.com/promis_misc/525444systematicreviewguide.pdf) (accessed on 12 September 2024).
25. Niknejad, N.; Ismail, W.; Ghani, I.; Nazari, B.; Bahari, M.; Che Hussin, A.R. Understanding service-oriented architecture (SOA): A systematic literature review and directions for further investigation. *Inf. Syst.* **2020**, *91*, 101491. [CrossRef]

26. Page, M.; McKenzie, J.; Bossuyt, P.; Boutron, I.; Hoffmann, T.; Mulrow, C.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. Research methods and reporting. *BMJ* **2021**, *372*, n71. [[CrossRef](#)]
27. *ISO/IEC 27001:2005*; Information Technology—Security Techniques—Information Security Management Systems—Requirements. International Organization for Standardization (ISO): Geneva, Switzerland, 2005.
28. *ISO 31000:2009*; Risk management—Principles and Guidelines. International Organization for Standardization (ISO): Geneva, Switzerland, 2018.
29. *ISO 31000:2018*; Risk Management—Principles and Guidelines. International Organization for Standardization (ISO): Geneva, Switzerland, 2018.
30. *BS 7799-1:2005*; Code of Practice for Information Security Management. British Standards Institution (BSI): London, UK, 2005.
31. Chobanov, V. Enhancing Resilience in Interconnected Cyber-Physical Power Networks. In Proceedings of the 7th International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2023, Ankara, Turkey, 26–28 October 2023. [[CrossRef](#)]
32. *ISO/IEC 27005: ISO/IEC 27005:2022*; Information Security, Cybersecurity and Privacy Protection—Guidance on Managing Information Security Risks. International Organization for Standardization (ISO): Geneva, Switzerland, 2022.
33. International Society of Automation. Security of Industrial Automation and Control Systems: An Overview of ISA/IEC 62443 Standards. ISA Global Cybersecurity Alliance. 2024. Available online: <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards> (accessed on 12 August 2024).
34. *NIST SP 800-82: National Institute of Standards and Technology*; Guide to Industrial Control Systems Security. NIST Special Publication (SP) NIST SP 800-82: Gaithersburg, MD, USA, 2022.
35. Ghani, H.; Luna Garcia, J.; Petkov, I.; Suri, N. User-centric security assessment of software configurations: A case study. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8364, pp. 196–212. [[CrossRef](#)]
36. Bartusiak, A.; Lassig, J.; Nicolai, S.; Bretschneider, P. Extended Gap Analysis: An Approach for Security Assessment of Critical Infrastructures. In Proceedings of the SEST 2022—5th International Conference on Smart Energy Systems and Technologies, Eindhoven, The Netherlands, 28 September 2022. [[CrossRef](#)]
37. Bartusiak, A.; Kühne, M.; Nitschke, O.; Lässig, J.; Nicolai, S.; Bretschneider, P. First step into automation of security assessment of critical infrastructures. *Sustain. Energy Grids Netw.* **2023**, *36*, 101139. [[CrossRef](#)]
38. Zhao, J.; Wu, D. The risk assessment on the security of industrial internet infrastructure under intelligent convergence with the case of G.E.'s intellectual transformation. *Math. Biosci. Eng.* **2022**, *19*, 2896–2912. [[CrossRef](#)]
39. Bobbert, Y.; Scheerder, J. Zero Trust Validation: From Practice to Theory: An empirical research project to improve Zero Trust implementations. In Proceedings of the 2022 IEEE 29th Annual Software Technology Conference, STC 2022, Gaithersburg, MD, USA, 3–6 October 2022; pp. 93–104.
40. Chatterjee, D. Should executives go to jail over cybersecurity breaches? *J. Organ. Comput. Electron. Commer.* **2019**, *29*, 1–3. [[CrossRef](#)]
41. Wessels, M.; van den Brink, P.; Verburgh, T.; Cadet, B.; van Ruijven, T. Understanding incentives for cybersecurity investments: Development and application of a typology. *Digit. Bus.* **2021**, *1*, 100014. [[CrossRef](#)]
42. Uchendu, B.; Nurse, J.R.C.; Bada, M.; Furnell, S. Developing a cyber security culture: Current practices and future needs. *Comput. Secur.* **2021**, *109*, 102387. [[CrossRef](#)]
43. Perera, S.; Jin, X.; Maurushat, A.; Opoku, D.-G.J. Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. *Informatics* **2022**, *9*, 28. [[CrossRef](#)]
44. Salin, H. Thrifty Guardians: Overcoming the Challenges of Establishing Security Champions on a Limited Budget. In Proceedings of the 2023 49th Euromicro Conference on Software Engineering and Advanced Applications, SEAA 2023, Durres, Albania, 6–8 September 2023; pp. 207–214. [[CrossRef](#)]
45. Abu Othman, N.A.; Norman, A.A.; Mat Kiah, M.L. Information System Audit for Mobile Device Security Assessment. In Proceedings of the 2021 3rd International Cyber Resilience Conference, CRC, Langkawi Island, Malaysia, 29–31 January 2021; p. 9392468. [[CrossRef](#)]
46. Butcher, D.S.; Brigham, C.J.; Berhalter, J.; Centers, A.L.; Hunkapiller, W.M.; Murphy, T.P.; Palm, E.C.; Smith, J.H. Cybersecurity in a Large-Scale Research Facility—One Institution's Approach. *J. Cybersecur. Priv.* **2023**, *3*, 191–208. [[CrossRef](#)]
47. Imbaquingo-Esparza, D.; Díaz, J.; Ron Egas, M.; Fuertes, W.; Molina, D. Information Security at Higher Education Institutions: A Systematic Literature Review. *Commun. Comput. Inf. Sci.* **2022**, *1648*, 294–309. [[CrossRef](#)]
48. Al-Emran, M.; Deveci, M. Unlocking the potential of cybersecurity behavior in the metaverse: Overview, opportunities, challenges, and future research agendas. *Technol. Soc.* **2024**, *77*, 102498. [[CrossRef](#)]
49. Irmak, E.; Kabalci, E.; Kabalci, Y. Digital Transformation of Microgrids: A Review of Design, Operation, Optimisation, and Cybersecurity. *Energies* **2023**, *16*, 4590. [[CrossRef](#)]
50. Yeoh, W.; Liu, M.; Shore, M.; Jiang, F. Zero trust cybersecurity: Critical success factors and A maturity assessment framework. *Comput. Secur.* **2023**, *133*, 103412. [[CrossRef](#)]
51. Abd Majid, M.; Zainol Ariffin, K.A. Model for successful development and implementation of Cyber Security Operations Centre (SOC). *PLoS ONE* **2021**, *16*, e0260157. [[CrossRef](#)]

52. NIST SP 800-115: *National Institute of Standards and Technology; Technical Guide to Information Security Testing and Assessment*. NIST Special Publication (SP) NIST SP 800-115: Gaithersburg, MD, USA, 2018.
53. *ISO/IEC 15408-1:2022; Information Security, Cybersecurity and Privacy Protection—Evaluation Criteria for IT Security*. International Organization for Standardization (ISO): Geneva, Switzerland, 2022.
54. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. In *NIST Cybersecurity White Paper (CSWP) NIST CSWP 29*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2024. [CrossRef]
55. NIST SP 800-53: *National Institute of Standards and Technology; Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication (SP) NIST SP 800-53: Gaithersburg, MD, USA, 2023.
56. NIST SP 800-55: *National Institute of Standards and Technology; Performance Measurement Guide for Information Security*. NIST Special Publication (SP) NIST SP 800-55: Gaithersburg, MD, USA, 2014.
57. NIST SP 800-207: *National Institute of Standards and Technology; Zero Trust Architecture*. NIST Special Publication (SP) NIST SP 800-207: Gaithersburg, MD, USA, 2016.
58. NIST SP 800-124: *National Institute of Standards and Technology; Guidelines for Managing the Security of Mobile Devices in the Enterprise*. NIST Special Publication (SP) NIST SP 800-124: Gaithersburg, MD, USA, 2013.
59. Nicoletti, B.; Appolloni, A. Digital transformation in ecosystems: Integrated operations model and its application to fifth party logistics operators. *J. Glob. Oper. Strateg. Sourc.* **2024**. [CrossRef]
60. Howell, G.; Franklin, J.M.; Sritapan, V.; Souppaya, M.; Scarfone, K. *Guidelines for Managing the Security of Mobile Devices in the Enterprise (No. NIST Special Publication (SP) 800-124 Rev. 2)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023.
61. *ISO/IEC 27002: ISO/IEC 27002:2022; Information Security, Cybersecurity and Privacy Protection—Information Security Controls*. International Organization for Standardization (ISO): Geneva, Switzerland, 2022.
62. *ISO/IEC 27019: ISO/IEC 27019:2024; Information Security, Cybersecurity and Privacy Protection—Information Security Controls for the Energy Utility Industry*. International Organization for Standardization (ISO): Geneva, Switzerland, 2024.
63. PCI Security Standards Council. PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard Version 3.2.1. 2018. Available online: [https://listings.pcisecuritystandards.org/documents/PCI\\_DSS-QRG-v3\\_2\\_1.pdf](https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf) (accessed on 18 May 2024).
64. ISACA. COBIT for Small and Medium Enterprises. 2019. Available online: [https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/cobits-value-for-small-and-medium-enterprises?gad\\_source=1&gclid=CjwKCAjwvIWzBhAlEiwAHHWgvyb00ic4YhJzYg4E9tj76ByOJpZBtdkMcDr2TENfls1Zyx6-SxL\\_DbhoC6EsQAvD\\_BwE](https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/cobits-value-for-small-and-medium-enterprises?gad_source=1&gclid=CjwKCAjwvIWzBhAlEiwAHHWgvyb00ic4YhJzYg4E9tj76ByOJpZBtdkMcDr2TENfls1Zyx6-SxL_DbhoC6EsQAvD_BwE) (accessed on 14 June 2024).
65. Salamah, F.B.; Palomino, M.A.; Papadaki, M.; Furnell, S. The Importance of the Job Role in Social Media Cybersecurity Training. In Proceedings of the 7th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2022, Genoa, Italy, 6–10 June 2022; pp. 454–462.
66. Dart, M.; Ahmed, M. Evaluating Staff Attitudes, Intentions, and Behaviors Related to Cyber Security in Large Australian Health Care Environments: Mixed Methods Study. *JMIR Hum. Factors* **2023**, *10*, e48220. [CrossRef]
67. Suzic, B. Securing integration of cloud services in cross-domain distributed environments. In Proceedings of the 31st Annual ACM Symposium on Applied Computing (SAC '16), Pisa, Italy, 4–8 April 2016; pp. 398–405. [CrossRef]
68. Wynn, M.; Jones, P. Corporate Digital Responsibility and the Business Implications of Quantum Computing. *Adv. Environ. Eng. Res.* **2023**, *4*, 1–18. [CrossRef]
69. Wynn, M.; Jones, P. New technology deployment and corporate responsibilities in the metaverse. *Knowledge* **2023**, *3*, 543–556. [CrossRef]
70. *ISO/IEC 27001:2013; Information Technology—Security Techniques—Information Security Management Systems—Requirements*. International Organization for Standardization (ISO): Geneva, Switzerland, 2013.
71. *ISO/IEC 27001:2022; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements*. International Organization for Standardization (ISO): Geneva, Switzerland, 2022.
72. Tanriverdi, N.S.; Metin, B. Enterprise Information Security Awareness and Behavior as an Element of Security Culture During Remote Work. In *Remote Work and Sustainable Changes for the Future of Global Business*; Ali, M., Ed.; IGI Global: Hershey, PA, USA, 2021; pp. 119–138. [CrossRef]
73. Metin, B.; Duran, S.; Telli, E.; Mutlutürk, M.; Wynn, M. IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation That Engenders a Security Culture. *Information* **2024**, *15*, 55. [CrossRef]
74. ISACA/CMMI Resource Centre. CMMI Cybermaturity Platform. 2018. Available online: <https://cmminstitute.com/resource-files/public/marketing/document/cmmi-cybermaturity-platform> (accessed on 6 October 2024).
75. World Bank. *Sectoral Cybersecurity Maturity Model (English)*; World Bank Group: Washington, DC, USA, 2023; Available online: <http://documents.worldbank.org/curated/en/099062623085028392/P17263707c36b702309f7303dbb7266e1cf> (accessed on 3 October 2024).

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.