electronics

MDPI

Article

Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach

Khalifa AL-Dosari * and Noora Fetais

College of Engineering, Qatar University, Doha P.O. BOX 2713, Qatar
* Correspondence: 200704317@qu.edu.qa; Tel.: +974-55815856

Abstract: Information-technology (IT) security standards are regularly updated in a rapidly changing technological world to maintain pace with advanced technologies. This study was motivated by the realization that established IT risk-management frameworks might provide an adequate defence for small- and medium-sized enterprises (SMEs), especially those actively adopting new technologies. We reviewed that a dynamic IT risk-management framework, updated to reflect emerging technological changes, would offer improved security and privacy for SMEs. To evaluate this, we conducted a systematic literature review spanning 2016 to 2021, focusing on IT risk-management research in various application areas. This study revealed that, while established frameworks like NIST have their benefits, they need to be better suited to the unique needs of SMEs due to their high degree of abstractness, vague guidelines, and lack of adaptability to technological advancements. The findings suggest a pressing need to evolve IT risk-management frameworks, particularly by incorporating advanced methods such as system dynamics, machine learning, and technoeconomic and sociotechnological models. These innovative approaches provide a more dynamic, responsive, and holistic approach to risk management, thereby significantly improving the IT security of SMEs. The study's implications underscore the urgency of developing flexible, dynamic, and technology-informed IT risk-management strategies, offering novel insights into a more practical approach to IT risk management.

Keywords: cybersecurity; information security; risk management; risk assessment

Citation: AL-Dosari, K.; Fetais, N. Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics* **2023**, *12*, 3629. https://doi.org/10.3390/electronics12173629

Academic Editor: Carlos Serrao

Received: 29 April 2023
Revised: 26 July 2023
Accepted: 29 July 2023
Published: 28 August 2023

1. Introduction

Cyber and information security are the need of the hour for SMEs because society and the economy have become more data-driven and managers are focusing on creating value-based services for their clients [1]. However, information is a critical asset and organizations are underinvesting in its protection. The rapid development of new technologies and the widespread use of cloud computing and platform-based services are creating more and more advancements in information systems [2]. It follows that the vulnerability of computer networks also increases and it is not trivial to address this in an increasingly complex system with interdependent components [3]. The role of digital technologies has been further grown following the COVID-19 pandemic, which puts more pressure on organisations with weaker security policies for information-technology (IT) systems. At the same time, there exist a variety of risk-management frameworks that are aimed to help organisations in assessing and managing cybersecurity risk [4].

Maintaining pace with the transformational shifts is crucial in a rapidly evolving technological era, particularly for the SMEs that need security and privacy. However, existing information-technology (IT) security standards often need more dynamism, proving to be a critical challenge for SMEs attempting to leverage new technology [5]. Not only are the current standards failing to address the complexities of advanced technology, but their implementation also brings high costs and lesser efficacy in IT risk management [2,6]. As

digitalisation expands, organisations face an escalating number of IT threats, a scenario that has been particularly aggravated in the post-COVID-19 landscape [7–9]. The limitations of existing IT risk-management frameworks are becoming increasingly evident, with significant drawbacks including outdated methodologies, complicated implementation processes, excessive focus on compliance, and the need for hybrid approaches to bridge gaps between controls and compliance requirements [10,11]. This situation warrants a thorough assessment of the effectiveness of current IT risk-management frameworks.

The issue becomes even more prominent in the context of small- and medium-sized enterprises (SMEs), for which the costs of implementing security standards are prohibitively high. The "one-size-fits-all" approach of existing frameworks often fails to accommodate SMEs' unique processes and needs, leading to higher administrative costs during implementation [12]. Hence, there is an urgent need for adaptable, cost-effective risk-management solutions that navigate the evolving technological landscape [13–15]. Despite several recent studies on IT risk management, the literature reveals a significant gap, with most studies focusing on specific contexts such as cloud computing, SMEs, or ISO/IEC 27001 and failing to provide a broad overview of the efficacy of existing IT risk-management frameworks [1–3,6,16–19]. This lack of systematic analysis creates a compelling research problem, to which this paper responds.

One of the reasons why SMEs in developing countries need help to grow and remaining sustainable is their inability to manage risks effectively. This could be explained by the limited guidelines available on pillars and underlying principles for risk management and information systems and the mapping of the factors that drive risk management in SMEs, despite decision makers' attempts to tackle the root causes of security failure, including access to financing and technology, as well as a regulatory environment for SMEs. Therefore, there is still an inadequate development of risk management and information systems in SMEs [20]. Internal control affects an organisation's efficiency by increasing the availability of high-quality information and reducing inappropriate behaviour [21]. Additionally, SMEs could not function effectively and efficiently without having a good form of information system in place [22].

Existing literature reviews on IT risk management and risk-assessment frameworks have primarily focused on specific environments and contexts. However, a comprehensive study of the recent literature across various sectors, including public administration, academia, business, and management, can provide valuable insights. This study examines various sources from computer science, cybersecurity, security standards, security management, and security frameworks. The proposed approach involves identifying previous literature reviews to contextualize this paper within the existing body of research, examining studies that compare multiple IT risk-management frameworks, and investigating studies focusing on a single framework; covering both established a framework. The research problem is to assess the adequacy of established IT risk-management frameworks in addressing organisations' challenges. The contributions of this study to the existing literature include providing a detailed understanding of the current state of IT risk management, identifying potential gaps or limitations in established frameworks, and offering recommendations for future research and development for SMEs. By addressing these issues, this study aims to enhance the effectiveness and adaptability of IT risk-management frameworks for organisations operating in diverse contexts and facing various risk-management challenges. Therefore, the study aims to bridge this gap, providing a holistic evaluation of the effectiveness of established IT risk-management frameworks across various contexts, and emphasising their applicability and cost-effectiveness for SMEs.

- How does an IT risk-management framework enhance the security standards across information systems in SMEs?
- What is necessary to establish an effective IT risk-management framework in SMEs?
- How are emerging IT risk-management frameworks addressing the shortcomings of established standards for SMEs?

The rest of the paper is structured as follows. Section 2 presents the related work covering system security specification and existing studies on IT risk management. Section 3 describes major IT risk-management frameworks. Section 4 outlines the research methodology that was used in conducting the systematic literature review. Section 5 presents a comparison of the effectiveness of cybersecurity risk frameworks. Section 6 presents information on studies that focused on a single existing or newly developed framework. Section 7 discusses the results of the survey and provides recommendations for future work. Finally, Section 8 concludes the findings of the study.

2. Literature Review

Because the current study is concerned with risk management, it is beneficial to review related literature on how to specify system security. Since the purpose of this study is to conduct a systematic review of the current literature, it is essential to look at evaluations of information-technology risk management that have been published in the last five years. The review that follows places the current research in context, allowing for easier comparisons with previous literature and highlighting the contributions of the current study to the field of psychology.

Cybersecurity and Information-Security Threats

The importance of robust IT risk-management frameworks for SEMs is overstated in today's increasingly digital and interconnected world. These frameworks are vital in identifying, assessing, addressing, and monitoring risks within information systems [23]. Adopting an established framework offers multiple benefits, including creating a prioritized roadmap toward improved IT security practices, fostering a common language for discussing IT risk challenges, setting security standards for future legal rulings, and promoting proactive IT risk management rather than reactive compliance [24]. However, the underlying concepts of security and risk are the bedrock upon which all IT security frameworks are built. The security of information systems is understood in terms of 'confidentiality, integrity, or availability' [25]. The landscape of IT security threats is vast and continually evolving. They can range from reconnaissance and information gathering to phishing attacks, creating spoof websites, producing counterfeit certificates, and delivering malware to internal information systems [26–29]. Such threats pose significant challenges to maintaining the security of information systems.

As for information security, it deals with preserving the confidentiality, integrity, and availability of information by applying risk-management procedures and assuring that the information is protected against unauthorized access, disclosure, alteration, destruction, and disruption [18]. Risk management involves identifying, assessing, and controlling threats to SMEs' digital assets, including information, networks, and systems [1]. Risk assessment, a significant part of risk management, involves identifying hazards, vulnerabilities and threat vectors, assessing the impact and probability of identified risks, and providing a basis for risk-mitigation decisions [23]. Despite the diverse risk-management frameworks available, their core objective remains to protect the SME's information assets by reducing risk to an acceptable level while maximizing the SME's business value [10].

Adversarial threats are defined as dangers originating from persons or organisations that wish to take advantage of the reliance on information systems and information resources [25]. Individuals are represented by outsiders or insiders, depending on their position. Competitive organisations, suppliers, partners, and customers are all examples of organisations. Accidental threats arise from erroneous actions taken by individual users or administrators. Structural threats correspond to equipment and control failures that occur due to circumstances outside of the expected operating parameters [26]. In particular, failures are caused by resource depletion, equipment ageing, or software malfunction. Structural threats cover storage, processing, communications, display, sensor, and controller equipment, as well as power supply, operating systems, networking, and mission-specific software. Finally, environmental threats describe natural disasters and failures of infras-

tructures that are external to the organisation but are critical to its operations [25]. This may include failure of telecommunications infrastructures, electrical power outages, and natural or man-made disasters such as fire, flood, hurricane, earthquake, and bombing.

3. Cybersecurity Risk-Management Frameworks

Small- and medium-sized enterprises (SMEs) face unique challenges in the contemporary business landscape, making risk management an essential focus [30]. The theoretical framework delineated in ([24], Figure 1) identifies five pivotal stages in risk management: identify (ID), project (PR), detect (DE), respond (RS), and recover (RC). At the identification stage, SMEs must ascertain potential threats and vulnerabilities, ranging from financial volatility and operational disruptions to cyber risks (Bannister and Remenyi, 2000). The projection phase requires businesses to anticipate identified risks' likelihood and potential impact [31]. Upon detection, timely recognition of emerging threats, especially in rapidly changing environments, is paramount [5]. Response mechanisms, both proactive and reactive, play a pivotal role in SMEs' ability to mitigate and manage risks [32]. Lastly, the recovery phase emphasizes the need for SMEs to bounce back postincidence, often requiring robust continuity plans and adaptability [33]. Across all these stages, the literature underscores the importance of a structured and comprehensive approach to risk management tailored to SMEs' unique needs and constraints.

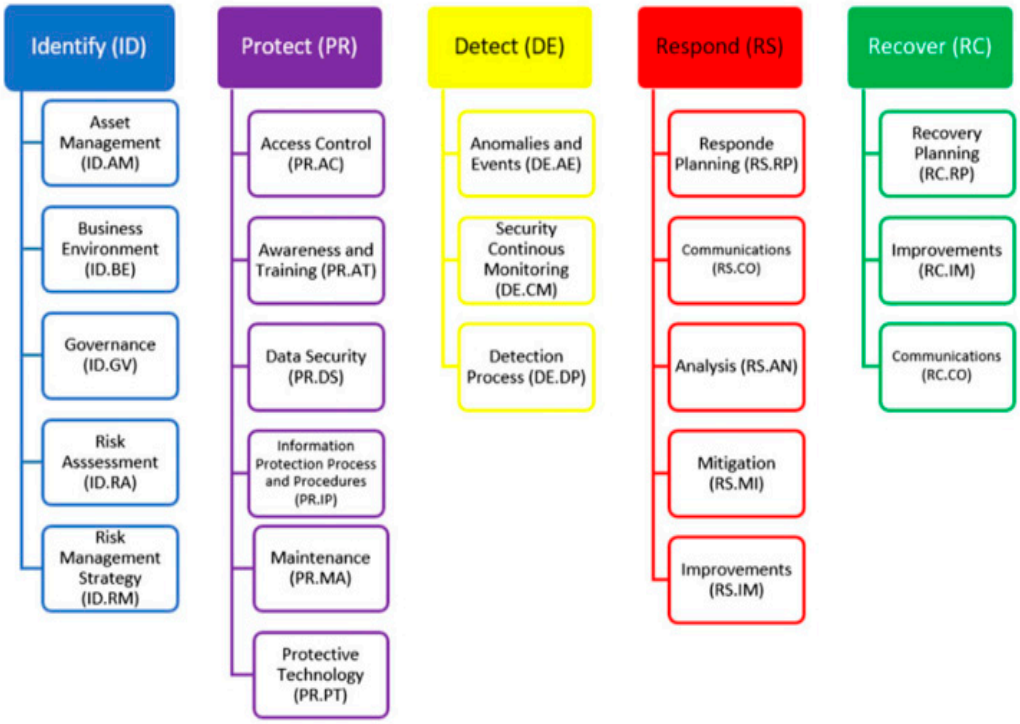

Figure 1. Structure of NIST SP 800-39 framework [24].

The relationship between information systems and organisational processes necessitates an integrated risk-management framework, offering a holistic approach to managing cybersecurity risks at an organisational level while considering the interconnections of the systems, processes, and employed information systems. The landscape of such frameworks is vast; however, two dominant ones commonly employed by organisations are from NIST and ISO. The NIST has offered pivotal contributions to IT security standards, with two exceptional standards being NIST SP 800-39 and NIST SP 800-30 (Revision 1). SP 800-39 provides a comprehensive blueprint for information-security risk management [8]. The standard's focus is managing risk at the organisational level, offering a consistent approach that allows for enhanced governance and an improved understanding of IT security impacts on SMEs' operations [23].

The objectives of the SP 800-39 standard are multifaceted. They emphasize the crucial role of IT risk management, advocate for the creation of robust governance processes, promote the application of risk management at various levels, and seek to foster a profound understanding of the effects of IT security risks on SME processes [26]. They also underscore the importance of accountability in decision-making related to cybersecurity risk management, emphasizing the importance of each stakeholder's role in maintaining a secure IT environment [27].

One of the key elements of the SP 800-39 is the multitiered structure of IT risk management [8]. Three major tiers are distinguished, as Tier 1 corresponds to the system level and describes strategic risk. The organisation decides on the risk-tolerance level which informs decision-making in lower tiers [34]. Tier 2 is associated with business processes and information flows given in ([26], Figure 2).

Figure 2. Multitiered structure of NIST SP 800-39 [26].

Tier 3 corresponds to information systems and tactical risk. Information flowing up allows top managers to better understand system-wide risks and adjust risk-tolerance policies accordingly. While this structure ensures that the risk executive function (REF) of the organisation is properly implemented, the NIST standard does not mandate any specific form of the REF. The REF allows stakeholders to direct resources in an excellent way that accounts for the strategic objectives of the organisation [25].

The SP 800-39 standard describes risk management in terms of four components, namely risk framing, risk assessment, risk-response strategy, and risk monitoring [34]. Risk framing aims to produce an actionable strategy for managing IT security risk. This step considers risk within the established environment which serves as the context for risk-based decision-making [27]. Risk framing identifies risk in terms of assumptions, constraints, tolerance, and priorities and trade-offs. In particular, risk tolerance is understood as the acceptable degree of risk [8]. Risk framing translates into a risk-management strategy which covers risk assessment, risk monitoring, and response strategies. The risk assessment step allows for identifying threats, vulnerabilities, potential damage, and likelihood of exploits. The SP 800-30 (Revision 1) standard is the corresponding NIST framework for IT security risk assessment. Finally, a risk-management strategy covers risk monitoring, which is responsible for consistent verification of compliance and assessment of the effectiveness of ongoing risk responses [35]. The risk-assessment component of risk management is

responsible for fully determining an IT security risk in terms of the likelihood of occurrence and the potential damage [23]. The standard contains information on preparing for and conducting a risk assessment as well as monitoring assessment processes. Risk assessment is linked to the three tiers of risk management described in the SP 800-39 standard [27]. The standards proposed by the International Organisation for Standardisation (ISO) and the International Electro Technical Commission (IEC), namely the ISO/ICE 27000 series, cover IT security. Most notably, the ISO/IEC 27005 standard describes information risk security. It proposes a continuous process of activity sequences that covers establishing context, assessing information, treating and monitoring risks, and informing the organisation's stakeholders [8]. Since the ISO/IEC 27005 standard only provides general guidelines for IT risk management, it can be applicable to a variety of organisations including SMEs, nonprofit organisations, and government agencies [36]. The key structural difference between it and the NIST standard is the lack of any specific recommended method for risk management. In addition to ISO/IEC 27005, the ISO/IEC framework provides policies and procedures to implement a holistic approach to establishing, monitoring, and improving IT security in accordance with general organisational risk management. A high-level overview of the ISO/IEC 27005 standard is shown in ([37], Figure 3) below.

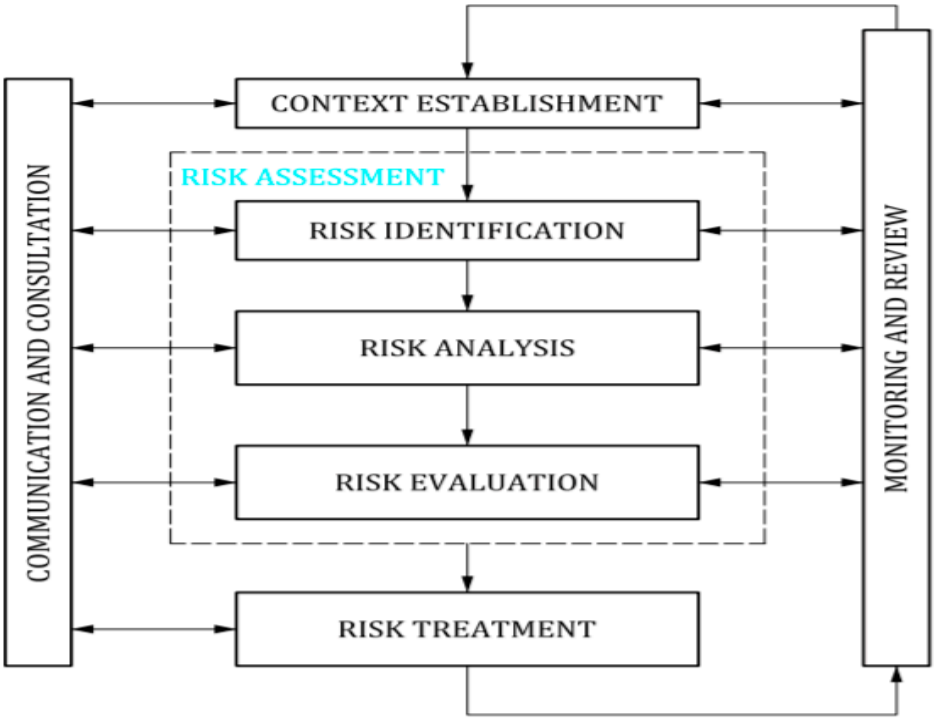

Figure 3. Structure of the ISO/IEC 27005 framework [37].

The graphic shown in [37], Figure 3 depicts how the International Organization for Standardization (ISO) uses an iterative approach to undertaking risk assessment [38]. First and foremost, the risk-management context should be established in order to specify the criteria for identifying risks, determining responsibility, determining consequences, determining the availability of information, and developing a methodology for evaluating risk impacts and likelihood [39]. The second step is risk assessment which comprises several stages, namely risk identification, risk analysis, and risk evaluation [37]. The iterative nature of the framework implies that the procedure of risk assessment is repeated if the information produced by previous a risk assessment is insufficient for making risk-management decisions [38]. For example, another iteration of the risk-assessment block is conducted with revised risk-evaluation or risk-impact criteria [37].

The result of risk assessment is a risk treatment which takes the form of avoiding, modifying, sharing, or retaining the risk [23]. The risk-treatment step is cyclical and

involves several procedures, including assessment of the treatment, estimation of residual risk levels, adjustment of the treatment in cases when residual risk levels are unacceptable, and assessment of the treatment's effectiveness (ISO 2018). This allows for changing context parameters, such as the risk-acceptance criteria, and producing another iteration of the treatment. The ISO 27005 framework emphasises that communication and consultation should be conducted throughout all steps of the risk-assessment process [37]. In particular, risks and treatments should be communicated to operational staff and managers to help mitigate risks and reduce potential damage. The framework specifies that the controls should be risk based. This captures the dynamic nature of risks and highlights the role of the risk-monitoring step. The standard also provides information on typical threats, constraints affecting organisation and scope, asset valuation, assessment of vulnerabilities, and risk modification (ISO 2018).

An alternative approach to establishing security requirements is incorporating them into requirements engineering as a part of project development. The Security Quality Requirements Engineering (SQUARE) methodology was developed at the Carnegie Mellon University (CMU) to provide a means for identifying and prioritising security requirements of IT systems [40]. The key advantage of this approach is that security concepts are built into the early development stages of the system [41]. The SQUARE model comprises nine key steps, including identification of safety and security goals, categorisation of requirements by level, and risk assessment, as well as prioritisation and inspection of requirements [42].

Surveys on IT Risk Management

The literature reviews [1,16] showed that established cybersecurity assessment frameworks are not well-suited for cloud computing. While recent research has investigated risks arising from using cloud services, it was suggested that the literature has paid little attention to risk assessment among cloud providers themselves. To address this gap, [16] proposed a new quantitative risk assessment model and found that evaluating cloud-platform risk requires dynamic models that would capture the degree of interconnectedness of complex cloud networks. It was noted that there is no consensus in the industry on how to assess cloud risks due to the lack of an appropriate framework and the dynamic nature of cloud systems. Similar findings for the IoT were reported [43]. It was noted that few quantitative approaches to cybersecurity risk management exist and that none of the established frameworks account for the IoT security ecosystem.

The literature review on the implementation of the ISO/IEC 27001 standard [18] suggested that there is a gap between the contributions of related studies and the requirements of the framework. The paper used semiquantitative analysis to identify research gaps. It was found that the majority of approaches offered in the related literature over the 2005–2018 period provide limited support in adopting the ISO/IEC 27001 standard. Furthermore, few of the examined studies considered the analysis and application of the risk-management system. The abstract nature of prominent IT security frameworks has been commonly noted to be a roadblock to implementing the guidelines in practice [18], which appears to be further exacerbated by the lack of research that would be relevant to practitioners. Similar findings were reported [3] from the surveyed the general academic literature on the ISO/IEC 27001 standard. The scholars noted that academia still perceives ISO/IEC 27001 as a technical topic and very little research exists that provides a managerial perspective. In a similar vein, the surveys [30,44] showed that the solutions provided in the academic literature lack empirical validation and real implementation. Furthermore, the literature was found to focus on common threats such as denial-of-service or phishing suggesting that there is a gap between emerging vulnerabilities and existing research. The gap was partially addressed [45] reporting that emerging threats are associated with the areas of cloud computing, IoT, and smartphones.

Several literature reviews focused on risk-management tools for SMEs [17] emphasised that SMEs lack resources for implementing available risk-management solutions. In particular, smaller firms have no dedicated personnel responsible for cybersecurity. The study developed

a new framework that contained essential policies for SMEs. Testing the framework in three case studies supported the effectiveness of the model. However, it was also noted that the framework should be complementary to established cybersecurity standards and frameworks. As such, the problem of implementing more complex 'one size fits all' systems, such as NIST, is still relevant. Similar findings for SMEs were reported [6,19]. Ref. [2] reviewed the literature for a specific case of IT security management in higher education institutions. The scholars used existing standards including ISO 27001, NIST, COBIT, and ITIL as a baseline to develop recommendations for creating a framework for such organisations. The problem of outdated standards was explored by [46] proposing new definitions for the information-security classification. The search was limited to publications from 2016 to 2021. The study targeted the Scopus database and Google Scholar for finding the studies on keywords "Cybersecurity Risk Management", "IT Risk Management", "Cybersecurity Risk Assessment", and "IT Risk Assessment". The data was gathered by collecting all research articles that were related to the security of information systems.

Table 1. Summary of existing surveys, their contributions, and limitations.

Reference	Contribution	Limitation
[1]	Developed a framework for IT risk management in cloud computing	Limited to cloud platforms
[17]	Developed a cyber-resilience framework with essential policies for SMEs	Limited to SMEs
[3]	Provides an overview of academic literature on the ISO/IEC 27001 standard	Limited to ISO/IEC 27001 standard
[2]	Provides recommendations for developing an IT risk framework for higher education institutions	Limited to higher education institutions
[19]	Identified a need for an effective risk-management framework for small businesses	Limited to SMEs
[6]	Little empirical research on IT risk management in SMEs	Limited to SMEs
[45]	Identified key emerging threats in cybersecurity	Focuses on emerging threats
[42]	Developed a four-layer IoT cyber risk-management framework	Focuses on IoT
[32]	Identified ISO/IEC 27001 as the prevalent model and found that implementation literature is severely lacking	Focuses on cybersecurity maturity models
[44]	Security approaches in the academic literature only focus on security in general; solutions need more empirical validation and real implementation	Focuses on mapping threats and vulnerabilities
[16]	Identified gaps in cloud risk assessment; proposed a quantitative risk-assessment model for cloud platforms	Limited to cloud platforms
[18]	Found limited support for ISO/IEC 27001 implementation in the academic literature	Limited to ISO/IEC 27001 standard
[10]	Identified insufficient research on recovering from incidents	Limited to NIST
[46]	Proposed updated definitions for information-security classification	Focuses on information-security classification
[47]	Review of IT risk assessment literature	Focuses on IT risk assessment; research dated only up to 2014

The extended literature suggests several focal points for exploring IT security risk management. Primarily, several studies target SMEs, revealing potential inadequacies of established frameworks that need to be more intricate or rigid for SMEs [8,48]. These findings hint at a chasm between conventional IT risk-management methodologies and SMEs' unique challenges. However, the applicability of these findings to larger organisations is questionable, thereby underscoring the need for an approach that transcends the size of organisations [7,17]. Simultaneously, other researchers focus narrowly on individual standards like ISO/IEC 27001 or NIST, which, although reflective of their pervasive use, can narrow the understanding of these standards' efficacy relative to their alternatives [17]. In contrast, our research embraces an array of IT security standards, aiming to furnish a more holistic comprehension of whether current risk-management frameworks effectively

respond to the practical requirements of organisations operating within various information systems. This integrated perspective can potentially offer crucial insights, driving the evolution of risk-management frameworks to be more adaptable, efficient, and effective for various organisations navigating the complex landscape of cybersecurity, information security, and risk management.

4. Research Methodology

4.1. Systematic Literature Review

This study employed a systematic literature review, a strategy renowned for its traceability and transparency, to scrutinize academic papers on risk management within SMEs. This methodology, extensively utilized in computer science and engineering, ensures a comprehensive and unbiased topic exploration. Key research phrases used during the review encompassed "Cybersecurity Risk Management", "IT Risk Management", "Cybersecurity Risk Assessment", and "IT Risk Assessment". Focusing on these critical elements in the broader field of risk management and information security systems, this study delivers a focused, in-depth examination of the prevailing discourse on IT risk in the contemporary information landscape.

4.2. Database and Population

With this study, we hope to find out how well-established information technology (IT) risk-management frameworks perform. Refs. [1–3,6,17,19,49] organized the literature review in the same manner. A wide range of sources is used to cover important articles from business, public administration, academia, and management, including papers from a variety of fields. The systematic literature review covers a variety of academic disciplines including cybersecurity, computer science, security standards, security management, and security frameworks. The search in the literature has been performed using such keywords as "Cybersecurity Risk Management", "IT Risk Management", "Cybersecurity Risk Assessment", and "IT Risk Assessment". The search was limited to publications from 2016 to 2021. Several publication databases are used, including Google Scholar, IEEE Xplore, Springer Link, Elsevier, and Science Direct. The study targeted the Scopus database and Google Scholar for finding the studies on the keywords "Cybersecurity Risk Management", "IT Risk Management", "Cybersecurity Risk Assessment", and "IT Risk Assessment". The data was gathered by collecting all research articles that were related to the security of information systems. The study used those articles and research papers which were related to the keywords "Cybersecurity Risk Management", "IT Risk Management", "Cybersecurity Risk Assessment", and "IT Risk Assessment".

4.3. Including and Excluding Criteria

The identified publications were organized into three main categories. The first category comprised the previous literature studies, serving as a benchmark to position our review within the existing body of literature. The second category includes the studies that conducted comparative analyses of various IT risk-management frameworks, which contributed to addressing the research questions Q1 and Q2. The final category focuses on the studies that examined a single framework and are further subdivided into those using an established framework and those developing novel models. These studies served to illuminate the research questions Q2 and Q3. As per our knowledge, there need to be more recent research articles and technical papers that encapsulate a comprehensive review of the literature on IT risk management from 2016 to 2022. Therefore, our review constitutes an important initiative towards systematically identifying the weaknesses of current IT frameworks and deciphering the essential features for future adaptations and emerging models.

4.4. Sample Size

Initially, 168 articles were found by the researcher using journal websites, the Scopus database, and Google Scholar. After that, 76 research articles were found to comply with

both the inclusion and the exclusion criteria and, from those, the most pertinent articles were chosen. Both papers that were identical to others and book reviews were removed from consideration. This particular investigation looked at a total of 29 different studies. Therefore, the study examined these 29 studies to determine what kind of writing and research has been done on risk management and information-security systems in SMEs. The 29 studies included those that had established SME risk management and information systems, frameworks, and models emphasizing the simplified risk-management framework implementation for SMEs. Additionally, the risk-management processes and marketing strategies were individually scrutinized to determine a commonality on the subject.

5. Findings of the Metadata

Ref. [20] compared several frameworks, including ISO/IEC 27001, NIST CSF, COBIT, OWASP, C2M2, ISO 22301, and ENISA [50,51]. It was argued that existing frameworks shared certain shortcomings that are becoming more and more challenging as the frequency of cyber-attacks continues to grow. First, these frameworks often require substantial implementation effort. For example, the NIST framework consists of almost 100 standards. The documentation for such frameworks can be overwhelming, which would likely translate into lower effectiveness of implemented risk-management tools. In other words, it can be challenging for organisations to employ established frameworks as guides for cybersecurity management which harms the adoption of universal frameworks and wastes organisational resources. Secondly, management of risk in information systems should shift from cybersecurity to cyber-resilience [52]. This reflects the focus on compliance in prominent frameworks, such as NIST, noted in similar research [16]. Cyber-resilience puts more emphasis on business continuity, the ability to prevent and recover from threats, and the capacity to adapt to the impacts of adverse events. Put differently, cybersecurity frameworks encourage a more reactive approach while cyber-resilience fosters a proactive mentality.

Ref. [53] makes a compelling argument for adopting hybrid IT risk-management frameworks, emphasizing that a balanced approach could provide superior outcomes. While the ISO 27000 series is recognized as an exceptional practice for comprehensive cybersecurity management, it could overwhelm certain cases with its exhaustive details. In such instances, a more straightforward framework like OCTAVE could provide an all-encompassing system that supplements ISO/IEC standards, filtering out inapplicable responses. Its simplified iteration, OCTAVE-S, could cater better to SMEs with a flat organisational structure [53]. Moreover, OCTAVE's operational uptime emphasis might be invaluable for manufacturing organisations. Ref. [53] postulates that blending a detailed standard such as ISO or NIST with a broader framework like OCTAVE could be optimal. Furthermore, integrating these risk frameworks with capability maturity modelling might facilitate easier alignment with finance and operational departments [54].

Considering specific threat types and vulnerabilities pertinent to an organisation's environment further enriches the analysis. Recognizing the role of behavioural factors in IT risk management and focusing on insider threats are particularly insightful [55]. Ref. [33] examined the risk assessment of insider threats across four frameworks: NIST, FRAP, OCTAVE, and CRAMM. They found NIST to be the most comprehensive, with each step tied to a distinct target and multiple management approaches. Concurrently, frameworks like FRAP and OCTAVE demand less time and resources, potentially boosting cybersecurity risk-management tool adoption among smaller organisations. Focusing on frameworks compatible with IoT services, identified a shortfall in NIST's automated risk quantification tools [56]. This diversity of research avenues and perspectives highlights the complexity and multidimensional nature of IT risk management in the context of cybersecurity, information security, and risk assessment.

Similarly, OCTAVE and TARA provided no quantification method for estimating recovery and risk impact. Meanwhile, ISO was reported to not have these weaknesses, although it may be too focused on compliance. Table 2 shows the summary of the studies discussed above.

Table 2. Summary of studies that compared existing IT risk-management frameworks.

References	Frameworks Compared	Findings
[53]	ISO 27001, OCTAVE, COBIT, NIST	No single framework that would fit all organisations; a hybrid approach is preferred that integrates risk frameworks with capability maturity modelling
[52]	ISO 27001, NIST CSF, COBIT, OWASP, C2M2, ISO 22301, ENISA	Existing frameworks require great implementation effort and have overwhelming documentation; a new cyber-resilience framework is needed that utilises machine learning
[23]	NIST, OCTAVE, ISO/IEC, FAIR, SABSA, CREF, CRMRF, COSO, ITIL, COBIT	Frameworks such as OCTAVE, FAIR, and AICPA may serve as enablers of cybersecurity risk management, complementing major NIST/ISO standards
[34]	NIST, FRAP, OCTAVE, CRAMM	NIST is the most well-formed framework for assessing insider threats
[56]	NIST, ISO/IEC, OCTAVE, TARA	Existing frameworks lack quantitative tools for estimating risk impact and risk likelihood
[35]	NIST, ISO	Users should choose the more convenient and affordable standard

In general, all the literature studies criticised the complexity and the lack of implementation guidelines for major IT risk-management frameworks. The results of the comparisons suggest that poor documentation increases the costs of implementation and reduces the effectiveness of risk-response measures. Several studies noted that a hybrid approach to risk management may be appropriate where an existing standard is complemented by additional models or enabling frameworks.

6. Comparative Analysis

An existing framework is explored in this study towards developing a new framework. Separating the two study groups allows for assessing the gap between existing frameworks and innovative solutions. It is possible that model extensions for specialized applications like cloud computing share the same flaws as the baseline model. In particular, the review of existing literature surveys suggests that academic literature treats the ISO/IEC standards as a theoretic construct and provides few implementation guidelines. As such, it can be valuable to separate the analysis of studies of new frameworks from that of established models.

The vast majority of recent literature has been focusing on extending prominent risk-management frameworks and applying them in specific cases, such as SMEs or cloud computing. It could be argued that it has been generally established that the existing standards are lacking, which translates into few recent studies that explicitly assess the effectiveness of basic frameworks such as NIST and ISO/IEC [3,18]. One example is the work by Benz and Chatterjee who proposed a tool for evaluating the maturity of SMEs according to NIST standards [8]. It was noted that NIST is insufficient for an SME IT leader. Most importantly, it was emphasised that implementing NIST can be overwhelming, as the framework is very complicated. Furthermore, NIST does not provide guidelines for acceptable ratings on each of the standards. SMEs may not have access to data from other organisations which prevents firms from gauging the effectiveness of implemented policies.

In addition, ref. [8] noted that NIST has no recommendations on best practices or directions for improvement. At the same time, it was argued that cybersecurity is still not universally recognised by SMEs as a high priority since executives may not see their businesses as likely targets of cyberattacks. This observation ties in with recent research that highlighted the role of behavioural factors in the effectiveness of IT risk management [57]. Similar findings on the shortcomings of NIST were reported [28]. The paper argued that NIST was too focused on compliance while quasi-quantitative scoring may give a false impression of rigour and accuracy, leading to lower effectiveness of IT risk management. Another study [29] considered effectiveness as perceived by investors. Cybersecurity awareness was associated with the perceived benefits of a risk-management framework.

The only study [27] that explicitly considered the effectiveness of an IT risk-management framework used the NIST framework with a cost–benefit model, which allowed for determining the cost-effective level of investing in IT security activities and selecting the most cost-effective direction for NIST implementation. It was shown that the cost-effectiveness of a NIST implementation depends on three key factors, namely the value of protected information, the probability of a security breach, and the productivity of the investment in IT security activities. The first two factors correspond to the NIST's definition of a risk, which emphasises the role of the expected damage following attachment and the likelihood of the attack. The presence of the third factor is more interesting and reflects the inability of NIST to capture the importance of human resources. The productivity of cybersecurity investments necessarily depends on human factors including leadership, trust, and behavioural biases. The paper [27] can be linked to recent research on the importance of cybersecurity awareness and trustworthiness in fostering proper security practices [55,58,59]. Table 3 shows the summary of studies that explored existing IT risk-management frameworks.

Table 3. Summary of studies that explored existing IT risk-management frameworks.

References	Frameworks Compared	Findings
[8]	NIST	SMEs have been lagging in their adoption of frameworks, such as NIST, due to the frameworks' complexity; an evaluation tool that is integrated with NIST may help encourage executives to pay more attention to cybersecurity risks
[27]	NIST	Cost-effectiveness of NIST depends on the value of information, likelihood of the breach, and productivity of cybersecurity investments
[28]	NIST	NIST is too focused on compliance; quasi-quantitative scoring may be misleading; out of date
[29]	AICPA	Perceived benefits of risk framework are associated with greater information quality and cybersecurity awareness

Overall, few recent studies have focused on assessing an established IT risk-management framework. The examined literature agrees on the existing standards being too complex and particularly challenging to adopt for smaller organisations.

Several studies focused on a specific area of application of cybersecurity risk management. For example, refs. [5,60] considered cybersecurity risk assessment for value-sensitive medical devices. The MDPC framework was used which adapted the NIST 800-30 standard to medical devices such as insulin pumps. The main idea behind the framework is the shift in perceiving information security as an asset rather than an obligation. However, the standard does not suggest any specific processes or criteria for matching risks with security controls. This shortcoming is shared with the underlying NIST framework and may be a significant roadblock to implementing cybersecurity risk management in complex systems. Nevertheless, the results [60] highlighted how the choice of the framework may articulate the value generated by investing in cybersecurity.

Few studies have considered causal relationships between security-related elements. Notably, [24] used systems dynamics to perform a dynamic and systemic assessment of cybersecurity risks in SMEs. Similar to [27,30,60,61], the employed risk-management framework was based on the NIST standard. More specifically, the Italian National Cyber Security Framework was created as a uniform approach to cybersecurity management for both SMEs and large companies. However, it extends NIST by considering priority levels and maturity levels for organisations and processes. The key result of [24] is illustrating how the benefits of addressing certain threats may systemically propagate to other security

components. Nevertheless, the paper did not empirically validate the identified causal relationships which further highlights the gap between available simulation and empirical studies. A more recent paper by [24] expanded on this approach and proposed a new tool for IT risk assessment that relied on the system dynamics methodology. The new SME Cyber Risk Assessment (SMECRA) framework was suggested to address dynamic organisational complexity. This should allow for assessing risks and related processes that vary over time which ties in with other research highlighting the need for dynamic assessment in such areas as cloud computing [16]. A simpler approach was used [48,62], adapting the NIST and ISO/IEC 27001 standards to manage cybersecurity risk in SMEs.

Further exploring how academics have tackled the issue of IT risk management in cloud computing reveals that it is necessary to account for risk economic qualification in a holistic technoeconomic model. This [7] proposed how to design an effective, agile, and automatic model of cybersecurity risk assessment for cloud computing which would allow for industrialising risk economic evaluation. Notably, the study found that the three most compliant established models present just below 60 percent of compliance of a theoretical reference model. This suggests that even considering the overlap across major risk-management frameworks, there is a gap of more than 40 percent that should be addressed by future models. Since it may not be clear which of the remaining vulnerabilities have the highest priority, a multicriteria decision analysis tool could be used to conduct a prioritised gap analysis. This [63] developed the CyFEr framework based on the empirical paradigm. The framework can use any base set of standards as controls input, such as NIST or C2M2. The research can be an important step towards better guidelines for implementing complex frameworks as well as automated risk assessment due to the prioritised vulnerability mitigation analysis. Entities that only enact these procedures because of the introduction of the GDPR will almost certainly use the ready-made (template) solutions that are made available by SMEs for risk assessment. This, of course, does not imply that the absence of consideration of the International Organization for Standardization is equivalent to poor quality in the analyses being conducted. On the other hand, one must always be prepared for the possibility that they deviate, albeit only slightly, from the globally recognized standards.

Several studies have highlighted the role of behavioural influences when considering the effectiveness of cybersecurity risk assessment and management. This is consistent with prominent frameworks such as NIST SP 800-39 and SP 800-30 failing to explicitly acknowledge the role of human resources in information systems. Ref. [57] integrated a human-behaviour model into cybersecurity risk assessment. This was aimed to facilitate communication so that users understand and promote informed judgement. It was noted that it may be insufficient to supply accurate risk information for producing an effective risk-management system. Individuals should be able to process and comprehend the risk message so that they may act on it in an informed way. This ties in with the Job Characteristics Model, suggesting that certain task features may foster a sense of responsibility and improve performance [57]. Furthermore, the Health Belief Model predicts that higher risk awareness promotes active engagement.

Only [64] explicitly studied the effectiveness of IT risk management. A new model was developed based on fuzzy set theory and machine-learning classifiers. Experimental results suggested that predicting risk types and estimating asset criticality using these tools leads to an effective risk-management practice. However, the paper was limited to cyber–physical systems. A more general approach was used [65] which proposed an architecture for integrating such frameworks as OCTAVE, NIST, ISO, CVSS, CMMI, TARA, and FAIR. It was found that FAIR promoted quantitative risk-based assessment of losses, while NIST and ISO were the most advanced frameworks offering standards for disaster recovery. Ref. [66] capitalised on the quantitative focus of FAIR and extended it using Bayesian networks. It was found that the extended model was more accurate and flexible. Meanwhile, the degree of interconnectedness in IoT and the lack of recovery planning in most of the frameworks could become a significant issue in the future as the adoption of

new technologies continues to grow [65]. The summary of studies that developed new IT risk-management frameworks is shown in Table 4.

Table 4. Summary of studies that developed new IT risk-management frameworks.

References	Focus	Framework	Findings
[60]	Value-sensitive design; medical devices	MDPC framework (extension of NIST 800-30)	Developed framework adapts the NIST framework to value-sensitive systems; the framework articulates the value created by cybersecurity risk management
[24]	SMEs; causality; system dynamics	Italian National Cyber Security Framework (extension of NIST)	Developed a causal mapping of IT risk categories
[67]	SMEs; causality; system dynamics	SME Cyber Risk Assessment (extension of NIST)	Developed a new system dynamics management framework suitable for dynamic organisational complexity
[61]	Cloud computing	Extension of NIST	Developed a cyber resilient capability maturity model for cloud computing
[7]	Cloud computing	Cloud Risk Assessment Model	Developed a cloud risk-assessment model by utilising technoeconomic models
[57]	SMEs	Sociotechnical framework for risk assessment	Introducing human element into risk assessment may improve communication within the company and with outside security experts
[63]	Multicriteria decision making	CyFEr	Developed a framework based on an empirical paradigm
[64]	Effectiveness	CRSM based on fuzzy logic/machine learning	
[68]	Cost analysis	Cost-based	Cybersecurity performance can be continuously improved by considering a cost-based approach to managing risk
[60]	Maturity model	Extension of NIST	Developed a capability maturity model using risk register for threat intelligence
[65]	IoT	FAIR, CMMI, CVSS, NIST, OCTAVE, TARA	Proposed an architecture for integrating existing frameworks
[69]	Risk assessment	AVARCIBER	Developed a risk-assessment framework
[36]	Risk management	Extension of ISO 27005, ISO 27002, ISO 27011, OCTAVE, NIST 800-30, OWASP	Developed a risk-management framework
[70]	Multisector model	Extension of ISO 27001, ISO 27005	Developed a risk-management framework that captures multisectoral interdependencies
[62]	SMEs	Extension of NIST	Designed a NIST-based risk-management framework focused on SMEs
[66]	Bayesian networks	Extension of FAIR	Developed a FAIR-based framework utilising Bayesian networks that are better performing
[71]	Automotive firms	STRIDE	Developed a framework for managing cybersecurity risk in the automotive industry
[48]	SMEs	Extension of ISO 27001	Designed an ISO-based risk-management framework focused on SMEs
[72]	Communication data	Extension of ISO/IEC 27005, NIST SP 800-30	Designed a framework for communication data applications

The NIST framework and its variants are the most frequently extended or adapted models across the studies, with at least 8 out of 19 papers leveraging it. Refs. [24,60] notably developed extensions of the NIST framework to cater to specific domains, while [44,62] focus specifically on SMEs. This underscores the flexibility and broad applicability of the NIST framework, with researchers continually finding it valuable for different contexts. A broad range of risk domains is under examination, including cloud computing, SMEs, IoT, multicriteria decision-making, and even automotive firms. This reflects the expanding universe of cybersecurity challenges that modern enterprises face. Studies [7,61] offer

specialized frameworks for the rapidly growing field of cloud computing. Advanced mathematical and computational techniques, such as system dynamics, Bayesian networks, fuzzy logic, and machine learning, are being integrated into risk-management frameworks. FAIR-based framework using Bayesian networks [66] CRSM with fuzzy logic/machine learning signify the growing intersection of artificial intelligence and risk management [64].

There is a noticeable shift toward recognizing the sociotechnical dimensions of cybersecurity. Ref. [57] emphasizes that integrating the human element can enhance risk communication. There is an evident interest in integrating various existing frameworks, as seen in [65]. This integrative approach recognizes the strengths of different frameworks and seeks to synthesize them for comprehensive risk management. Several studies [24,48,62] specifically target SMEs. This focus underscores SMEs' unique risk-management challenges, as opposed to larger enterprises, and the need for tailored approaches.

7. Discussion

Recent studies have underscored a pressing discord between prevailing IT risk-management frameworks and the actual security requirements of organisations. While multiple adaptations and novel frameworks have emerged to bridge evident gaps in IT risk assessment and management, there is a lingering apprehension that these nascent solutions might echo the shortcomings intrinsic to their well-established counterparts. At the heart of this concern is the oft-debated applicability of such frameworks, especially for small- and medium-sized enterprises (SMEs). When juxtaposed with the often-scant IT security budgets of SMEs, the financial burden of adopting intricate standards renders them disproportionately costly [45]. This financial strain stems from the inflexibility of generic, "one size fits all" frameworks, notably the NIST, which frequently require modifications beyond the capabilities or needs of SMEs [6].

Despite its pervasive utilization across IT security risk management, the NIST standard has been critiqued for its inherent qualitative nature, often rendering its guidelines more theoretical than actionable [19]. A prominent critique highlighted targets the risk-assessment component of the NIST standard [16]. While it mandates estimations of threat likelihood and the potential consequences of untoward events, it conspicuously needs lucid directives on the estimation procedures. More than a mere oversight, this deficiency has implications for operational effectiveness and could lead to inconsistencies in risk assessments across different SMEs. Ultimately, while the NIST framework provides a panoramic view of risk management's primary constituents, it fails to deliver precise, actionable solutions tailored to IT security challenges. As risk assessors strive to delineate concrete concepts such as weaknesses, threats, and vulnerabilities, they would significantly benefit from a more prescriptive framework that fuses NIST's theoretical robustness with practical guidelines and adaptability.

The dominant standards explain risk assessment too abstractly and give little guidance for implementation [16]. This is important for applying standards to cloud settings, which are highly interdependent and continually changing [23]. As a result, measuring cloud hazards using qualitative or semiquantitative scales is ambiguous [3]. Another outstanding factor has been found that due to the complexity of IT risk management in the presence of multiple cloud service providers; recent research appears to have focused on the organisation in question while ignoring the supplier network and security interdependencies [16]. At the same time, established frameworks for cloud security, such as QUIRC, OPTIMIS, and CSPRAM may become too complex and unmanageable if users are involved in all stages of risk assessment. Another possible issue with NIST is the large number of related standards [23]. The overarching SP 800-39 framework requires complementary guidance documentation such as SP 800-37 and SP 800-30 [17]. It can be challenging for organisations to achieve a clear understanding of the whole framework and to extract information that is relevant to the organisation's processes and security risks [64]. SMEs are more likely to encounter this problem and face higher relative costs of implementing the standard, which is a shortcoming shared by a "one size fits all" approach to risk management [6,19].

The findings from the reviewed studies have provided strong insights into the research questions. This study discusses the results concerning each research question.

1. *How does the IT risk-management framework enhance the security standards across information systems in SMEs?*

IT risk-management frameworks play a crucial role in enhancing the security standards across information systems in SMEs by providing structured and systematic approaches to identifying, assessing, and managing potential risks. Studies highlighted the importance of established frameworks like NIST and ISO/IEC in providing baselines for effective risk management [8,28]. However, the complexity of these frameworks has been noted as a potential deterrent, especially for SMEs with limited resources [8]. Customizing and adapting these frameworks to the specific context of SMEs could enhance their applicability and effectiveness. In particular, refs. [27,73] illustrated how frameworks, such as NIST, can be adapted and expanded to suit the needs of SMEs better, indicating that flexibility and adaptability are crucial elements in enhancing security standards.

2. *What is necessary to establish a practical IT risk-management framework in SMEs?*

Several necessary elements were identified to establish a practical IT risk-management framework in SMEs. These include the simplicity of implementation, flexibility and adaptability of the framework to specific needs, clear guidelines for improvement, and the acknowledgement of the human aspect of cybersecurity. Simplicity and usability were considered critical, with established frameworks like NIST viewed as complex and overwhelming for SMEs [8]. A need for clear guidelines and best practices was also identified to facilitate SMEs in implementing the framework effectively [8]. Additionally, several studies emphasized the importance of acknowledging human factors in developing a practical IT risk-management framework. The importance of including human behaviour and awareness in risk management was notably discussed [57] indicating the necessity of frameworks that focus on not only technical aspects but also the human elements of cybersecurity.

3. *How are emerging IT risk-management frameworks addressing the shortcomings of established standards for SMEs?*

Emerging IT risk-management frameworks primarily address established standards' shortcomings by focusing on specific application areas, integrating human behavioural aspects, and offering more dynamic and adaptable approaches. For instance, ref. [67] developed the SME Cyber Risk Assessment (SMECRA) framework that addresses dynamic organisational complexity, indicating an emerging focus on the need for frameworks that can adapt and respond to changes over time. In terms of specific areas of application, studies [7,60] focused on value-sensitive medical devices and cloud computing, respectively, highlighting an increasing focus on domain-specific risk-management frameworks.

Additionally, several new frameworks have started integrating human-behaviour models into cybersecurity risk assessment [57], addressing the human-factor shortcoming identified in established models. In conclusion, the ongoing research in IT risk management is leaning towards more specialized, dynamic, and human-centred frameworks, addressing the known shortcomings of established standards and better meeting the needs of SMEs.

7.1. Practical Implications

Existing frameworks' silo approach may positively influence risk management of IT systems that use emerging technologies like cloud networks in SMEs. Indeed, this approach indicates that standards analyse a single environment, such as a cloud service provider or a client, while neglecting supply-chain network interdependencies [16]. This increases risk exposure which translates SMEs' security standards into lower effectiveness of the risk-management framework. New technologies are rapidly advancing and require a more dynamic approach to risk assessment [18]. The gap also highlights the importance of SMEs conducting due diligence on their partners and third-party vendors due to the

increasing complexity and interdependence of IT systems. One possible direction for future research is to consider technology-enabled automation in these SMEs [6]. Automated risk assessment in those SMEs would allow for a more proactive approach to risk mitigation due to the ability to dynamically monitor cybersecurity threats and vulnerabilities [46]. This approach would be suitable for newer technologies, such as cloud computing, which involves indirect assets harmed only through adverse impacts on other assets. Automated tools may also facilitate the shift from qualitative or semiquantitative frameworks, such as NIST, to quantitative assessment that captures the impacts on business losses and costs to recover from an attack [17].

In addition, small and medium enterprises (SMEs) must conduct risk assessments to identify and mitigate IT security risks effectively. This involves identifying the vulnerabilities, threats, and potential impacts of each aspect of their IT infrastructure. Understanding what risks exist is critical to the ability to counteract them. Once the risks have been identified, it is essential to establish a robust cybersecurity framework that aligns with globally recognized standards such as ISO 27001 or the NIST framework. The cybersecurity framework should provide guidelines and procedures to prevent, detect, and respond to cybersecurity risks. Simultaneously, SMEs must invest in relevant security tools such as firewalls, antivirus software, encryption tools, and intrusion detection systems. These tools will help to protect the organisation's data and IT resources from malicious activities.

Moreover, human error or negligence can often be a significant source of security incidents. Therefore, conducting regular staff training on cybersecurity best practices is crucial. Employees must be made aware of common threats, such as phishing attacks and ransomware, and trained to respond effectively. In addition, SMES should review and update their IT policies and procedures regularly. Changes in technology, business environment, or regulatory requirements might necessitate adjustments to ensure ongoing relevance and effectiveness. Finally, having a well-defined and rehearsed incident response plan is another crucial step in mitigating IT security risks. The plan should outline how to respond to an IT security incident swiftly and efficiently to minimize damage and downtime. This also includes having a disaster recovery and business continuity plan to ensure operations can resume quickly after an incident.

All these strategies must be underpinned by a security culture where all stakeholders understand the importance of maintaining strong IT security practices. With an ongoing focus on security, SMEs can significantly reduce their IT security risks.

7.2. Theoretical, Managerial and Societal Implications

The findings from this study serve as a stepping stone in the continually evolving domain of IT risk management. The identified shortcomings and advantages of the established frameworks will stimulate further academic inquiries to address these gaps. It elucidates the dynamic interplay between technological evolution and IT risk-management practices, reinforcing the need for frameworks that can adeptly respond to a rapidly transforming digital landscape. This study fosters an interdisciplinary dialogue beyond the traditional IT security discourse by emphasizing system dynamics, machine learning, and sociotechnological models. Hence, it challenges the scholarly community to consider IT risk management as a static entity and a vibrant, complex system with inherent interactions and feedback loops. From a managerial perspective, this study underscores the necessity of selecting and implementing IT risk-management frameworks congruent with the SME's specific needs and the nature of its information systems. It encourages management to consider the costs and complexities associated with established frameworks, evaluate the efficacy of risk-management strategies, and contemplate the feasibility of emerging frameworks with advanced techniques. Societally, this study underscores the importance of robust IT risk-management practices in maintaining data integrity, privacy, and cybersecurity. By spotlighting the limitations of the current standards and advocating for adaptable, responsive risk-management practices, it aims to foster a safer, more secure digital society. This is particularly critical given the escalating

prevalence of digital channels in everyday life, the increasing reliance on interconnected systems, and the rising threats to information security.

8. Conclusions

The present survey aimed to assess the effectiveness of established IT risk-management frameworks in SMEs. A literature review was performed on IT risk-management research covering the 2016–2021 period, which also highlights the need for information-security standards in SMEs. While established IT risk-management frameworks, such as NIST and ISO, are foundational to enhancing the security of SMEs, their application has shortcomings. Issues related to high-risk uncertainty, subjective probability associations, and a semiquantitative assessment scale potentially contribute to inaccuracies in assessing IT security risks. An essential critique of these frameworks is their focus on compliance rather than proactive security, making them less suitable for smaller organisations. Furthermore, the assumed trustworthiness of entities related to the organisation and the predictability of their behaviour might only sometimes hold, underscoring the need for individualized assessments. These frameworks require continuous updates to cover threats associated with emerging technologies. Despite these limitations, such frameworks remain valuable tools for describing and prioritizing tasks necessary to manage security capabilities and assist in preparation for compliance and other IT audits. Ultimately, a successful risk-management program should enable SMEs to consider the range of risks they are exposed to and understand the potential impacts these could have on their strategic goals. In moving forward, it will be necessary for standards and frameworks to adapt to the changing landscape of IT security threats and for organisations to tailor their use of these frameworks to their specific context and needs.

In addition, the study offers SMEs a risk-management tool that is all encompassing and does not concentrate on a particular functional area or industry. This tool assesses the dimensions of risk within the context of SME information systems. According to the findings of this research, even though SMEs have scarce resources, it may still be possible for them to adopt a holistic approach to their risk management by managing the elements of information democracy. This would be a positive development. This may assist SMEs in risk assessment, reconciling their risk appetite, and utilizing risk-management systems and information systems for their survival and long-term viability. The fact that the research was only focused on internal information is one of its flaws; as a result, it is suggested that future studies examine the information available to the public. The results that were obtained provide an overview of the bigger picture regarding how the process of risk management operates in information security in SMEs. The benefits and drawbacks of utilizing this method are both brought to light here. It has become known that businesses do not place a great deal of importance on the human element of risk assessment or on locating potential hazards that are the result of the actions of workers. The findings of the research should encourage further assertion of businesses in the area of risk management. This will make it possible in the future to estimate this same rate of growth of business entities' knowledge within the scope of their use of suggestions derived from global standards.

Limitations and Future Directions

Despite the extensive literature on established and emerging IT risk-management frameworks, this study has limitations. The broad spectrum of rapidly developing new technologies was not adequately addressed. Thus, future research could focus on assessing the adaptability and effectiveness of these frameworks in response to specific emerging technologies such as AI, quantum computing, or blockchain. Furthermore, the research could explore the development of sector-specific or technology-specific risk-management frameworks to accommodate the unique vulnerabilities and threats inherent to them. Cross-sectoral comparisons also yield further insights into how different industries manage IT risk. Moreover, the cultural, geographical, and regulatory contexts of organisations, which may impact the implementation and effectiveness of these frameworks, could be investigated

in depth. While this study suggests incorporating advanced techniques, such as system dynamics and machine learning, into risk-management practices, more empirical studies are required to validate this proposition and explore its practical implementation. Finally, in the context of the increased prevalence of remote work and online transactions due to the pandemic, future studies could delve into the new set of IT risks and how risk-management frameworks can be adapted accordingly. Improving the overall language and readability of the manuscript is advised to ensure the information presented is accessible and engaging to academia and industry professionals.

Author Contributions: Conceptualization, K.A.-D. and N.F.; methodology, K.A.-D. and N.F.; investigation, K.A.-D. and N.F.; writing original draft preparation, K.A.-D.; writing—review and editing, N.F.; supervision, N.F. All authors have read and agreed to the published version of the manuscript.

Funding: For now, this research has received no external funding. However, it may be funded by the QNLP.

Data Availability Statement: The data can be shared upon request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Tissir, N.; El Kafhali, S.; Aboutabit, N. Cybersecurity management in cloud computing: Semantic literature review and conceptual framework proposal. *J. Reliab. Intell. Environ.* **2021**, *7*, 69–84. [CrossRef]
2. Merchan-Lima, J.; Astudillo-Salinas, F.; Tello-Oquendo, L.; Sanchez, F.; Lopez-Fonseca, G.; Quiroz, D. Information security management frameworks and strategies in higher education institutions: A systematic review. *Ann. Telecommun.* **2021**, *76*, 255–270. [CrossRef]
3. Culot, G.; Nassimbeni, G.; Podrecca, M.; Sartor, M. The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *TQM J.* **2021**, *33*, 76–105. [CrossRef]
4. Sulistyowati, D.; Handayani, F.; Suryanto, Y. Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *JOIV Int. J. Inform. Vis.* **2020**, *4*, 225–230. [CrossRef]
5. Putra, I.M.M.; Mutijarsa, K. Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005. In Proceedings of the 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT), Virtual, 9–11 April 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 14–19. [CrossRef]
6. Alahmari, A.; Duncan, B. Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 15–19 June 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–5. [CrossRef]
7. Bendicho, C. Cyber Security in Cloud: Risk Assessment Models. In *Intelligent Computing*; Springer: Cham, Germany, 2022; pp. 471–482. [CrossRef]
8. Benz, M.; Chatterjee, D. Calculated risk? A cybersecurity evaluation tool for SMEs. *Bus. Horiz.* **2020**, *63*, 531–540. [CrossRef]
9. Toapanta, S.M.T.; Bonilla, C.A.O.; Gallegos, L.E.M. Analysis of adequate security algorithms oriented to cybersecurity management for a distributed architecture. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020; IEEE: Piscataway, NJ, USA; pp. 715–721. [CrossRef]
10. Krumay, B.; Bernroider, E.W.; Walser, R. Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST Cybersecurity Framework. In *Nordic Conference on Secure IT Systems*; Springer: Cham, Germany, 2018; pp. 369–384. [CrossRef]
11. Renaud, K.; Flowerday, S.; Warkentin, M.; Cockshott, P.; Orgeron, C. Is the responsibilization of the cyber security risk reasonable and judicious? *Comput. Secur.* **2018**, *78*, 198–211. [CrossRef]
12. Kabanda, S.; Tanner, M.; Kent, C. Exploring SME cybersecurity practices in developing countries. *J. Organ. Comput. Electron. Commer.* **2018**, *28*, 269–282. [CrossRef]
13. Hajda, J.; Jakuszewski, R.; Ogonowski, S. Security Challenges in Industry 4.0 PLC Systems. *Appl. Sci.* **2021**, *11*, 9785. [CrossRef]
14. Nurse, J.R.; Radanliev, P.; Creese, S.; De Roure, D. If you can't understand it, you can't properly assess it! The reality of assessing security risks in Internet of Things systems. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT—2018, London, UK, 28–29 March 2018. [CrossRef]
15. Sobb, T.; Turnbull, B.; Moustafa, N. Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics* **2020**, *9*, 1864. [CrossRef]
16. Akinrolabu, O.; Nurse, J.R.; Martin, A.; New, S. Cyber risk assessment in cloud provider environments: Current models and future needs. *Comput. Secur.* **2019**, *87*, 101600. [CrossRef]
17. Carías, J.F.; Arrizabalaga, S.; Labaka, L.; Hernantes, J. Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs. *IEEE Access* **2021**, *9*, 80741–80762. [CrossRef]

18. Ganji, D.; Kalloniatis, C.; Mouratidis, H.; Gheytassi, S.M. Approaches to develop and implement iso/iec 27001 standard-information security management systems: A systematic literature review. *Int. J. Adv. Softw.* **2019**, *12*. Available online: http://www.iariajournals.org/software/ (accessed on 19 June 2023).
19. Tam, T.; Rao, A.; Hall, J. The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses. *Comput. Secur.* **2021**, *109*, 102385. [CrossRef]
20. Ndungo, J.M.; Rucha, K. Factors Affecting the Growth of Smes: A Study of Smes in Kajiado District. *Int. J. Financ.* **2017**, *2*, 58–75. [CrossRef]
21. Cheng, Q.; Goh, B.W.; Kim, J.B. Internal Control and Operational Efficiency. *Contemp. Account. Res.* **2018**, *35*, 1102–1139. Available online: https://ink.library.smu.edu.sg/soa_research/1210 (accessed on 19 June 2023).
22. Ki-Aries, D.; Faily, S. Persona-Centred Information Security Awareness. *Comput. Secur.* **2017**, *70*, 663–674. [CrossRef]
23. Giuca, O.; Popescu, T.M.; Popescu, A.M.; Prostean, G.; Popescu, D.E. A Survey of Cybersecurity Risk Management Frameworks. In *International Workshop Soft Computing Applications*; Springer: Cham, Germany, 2018; pp. 240–272. [CrossRef]
24. Armenia, S.; Angelini, M.; Nonino, F.; Palombi, G.; Schlitzer, M.F. A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decis. Support Syst.* **2021**, *147*, 113580. [CrossRef]
25. NIST, 2012. SP 800-30 Rev. 1. Guide for Conducting Risk Assessments. Available online: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (accessed on 8 July 2023).
26. Barret, M. *Framework for Improving Critical Infrastructure Cybersecurity*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018. [CrossRef]
27. Gordon, L.A.; Loeb, M.P.; Zhou, L. Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *J. Cybersecur.* **2020**, *6*, tyaa005. [CrossRef]
28. Maclean, D. The NIST risk management framework: Problems and recommendations. *Cyber Secur. A Peer-Rev. J.* **2017**, *1*, 207–217.
29. Yang, L.; Lau, L.; Gan, H. 'Investors' perceptions of the cybersecurity risk management reporting framework. *Int. J. Account. Inf. Manag.* **2020**, *28*, 167–183. [CrossRef]
30. Prasanna, B.L.; SaidiReddy, M. (CSM2-RA-R2-TI): Cyber Security Maturity Model for Risk Assessment Using Risk Register for Threat Intelligence. *J. Phys. Conf. Ser.* **2021**, *2040*, 012005. [CrossRef]
31. Abbass, W.; Baina, A.; Bellafkih, M. Using EBIOS for risk management in critical information infrastructure. In Proceedings of the 2015 5th World Congress on Information and Communication Technologies (WICT), Marrakesh, Morocco, 14–16 December 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 107–112. [CrossRef]
32. Rabii, A.; Assoul, S.; Touhami, K.O.; Roudies, O. Information and cyber security maturity models: A systematic literature review. *Inf. Comput. Secur.* **2020**, *28*, 627–644. [CrossRef]
33. Radziwill, N.M.; Benton, M.C. Cybersecurity cost of quality: Managing the costs of cybersecurity risk management. *arXiv* **2017**, arXiv:1707.02653.
34. Hashim, N.A.; Abidin, Z.Z.; Zakaria, N.A.; Ahmad, R.; Puvanasvaran, A.P. Risk Assessment Method for Insider Threats in Cyber Security: A Review. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 126–130. [CrossRef]
35. Salnyk, S.; Sydorkin, P.; Nesterenko, S.; Zaytcev, A.; Konotopetc, M. Comparative analysis of the us ISO and NIST standards on assessing the risk of information leakage in communication systems. *J. Sci. Pap. Soc. Dev. Secur.* **2020**, *10*, 29–39. [CrossRef]
36. Shirazi, A.; Kazemi, M. A New Model for Information Security Risk Management. In *ICT for an Inclusive World*; Springer: Cham, Germany, 2020; pp. 551–566. [CrossRef]
37. SIS. 2018. ISO/IEC 27005. Available online: https://www.sis.se/api/document/preview/80005503/ (accessed on 19 June 2023).
38. ISO. 2018. ISO/IEC DIS 27005 Information Security, Cybersecurity and Privacy Protection—Guidance on Managing Information Security Risks. Available online: https://www.iso.org/standard/80585.html (accessed on 13 July 2023).
39. Everett, C. A risky business: ISO 31000 and 27005 unwrapped. *Comput. Fraud. Secur.* **2011**, *2011*, 5–7. [CrossRef]
40. Mead, N.R.; Stehney, T. Security quality requirements engineering (SQUARE) methodology. *ACM SIGSOFT Softw. Eng. Notes* **2005**, *30*, 1–7. [CrossRef]
41. Suleiman, H.; Svetinovic, D. Evaluating the effectiveness of the security quality requirements engineering (SQUARE) method: A case study using smart grid advanced metering infrastructure. *Requir. Eng.* **2013**, *18*, 251–279. [CrossRef]
42. Fabian, B.; Gürses, S.; Heisel, M.; Santen, T.; Schmidt, H. A comparison of security requirements engineering methods. *Requir. Eng.* **2010**, *15*, 7–40. [CrossRef]
43. Lee, I. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet* **2020**, *12*, 157. [CrossRef]
44. Humayun, M.; Niazi, M.; Jhanjhi, N.Z.; Alshayeb, M.; Mahmood, S. Cyber security threats and vulnerabilities: A systematic mapping study. *Arab. J. Sci. Eng.* **2020**, *45*, 3171–3189. [CrossRef]
45. Hussain, A.; Mohamed, A.; Razali, S. A Review on Cybersecurity: Challenges Emerging Threats. In Proceedings of the 3rd International Conference on Networking, Information Systems Security, Marrakech, Morocco, 31 March–2 April 2020; pp. 1–7. [CrossRef]
46. Collard, G.; Ducroquet, S.; Disson, E.; Talens, G. A definition of information security classification in cybersecurity context. In Proceedings of the 2017 11th International Conference on Research Challenges in Information Science (RCIS), Brighton, UK, 10–12 May 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 77–82. [CrossRef]

47. Pan, L.; Tomlinson, A. A systematic review of information security risk assessment. *Int. J. Saf. Secur. Eng.* **2016**, *6*, 270–281. [CrossRef]
48. Antunes, M.; Maximiano, M.; Gomes, R.; Pinto, D. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *J. Cybersecur. Priv.* **2021**, *1*, 219–238. [CrossRef]
49. Ray, C.; Iphar, C.; Napoli, A. Methodology for Real-Time Detection of AIS Falsification. In *Maritime Knowledge Discovery and Anomaly Detection Workshop*; Publications Office of the European Union: Luxembourg, 2016; pp. 74–77.
50. ENISA. EBIOS Framework. 2021. Available online: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ebios.html (accessed on 12 July 2023).
51. Zahra, B.F.; Abdelhamid, B. Risk analysis in Internet of Things using EBIOS. In Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 9–11 January 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–7. [CrossRef]
52. Bejarano, M.H.; Rodríguez, R.J.; Merseguer, J. A Vision for Improving Business Continuity through Cyber-Resilience Mechanisms and Frameworks. In Proceedings of the 2021 16th Iberian Conference on Information Systems and Technologies (CISTI), Chaves, Portugal, 23–26 June 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–5. [CrossRef]
53. Aminzade, M. Confidentiality, integrity and availability–finding a balanced IT framework. *Netw. Secur.* **2018**, *5*, 9–11. [CrossRef]
54. Lundgren, M. Rethinking capabilities in information security risk management: A systematic literature review. *Int. J. Risk Assess. Manag.* **2020**, *23*, 169–190. [CrossRef]
55. Hadlington, L. The "human factor" in cybersecurity: Exploring the accidental insider. In *Research Anthology on Artificial Intelligence Applications in Security*; IGI Global: Hershey, PA, USA, 2021; pp. 1960–1977. [CrossRef]
56. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP J. Inf. Secur.* **2020**, *2020*, 8. [CrossRef]
57. Boletsis, C.; Halvorsrud, R.; Pickering, J.B.; Phillips, S.C.; Surridge, M. Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment. In *VISIGRAPP (3: IVAPP)*; SciTePress: Setubal, Portugal, 2021; pp. 266–274. [CrossRef]
58. Bada, M.; Sasse, A.M.; Nurse, J.R. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv* **2019**, arXiv:1901.02672.
59. Gundu, T. Acknowledging and reducing the knowing and doing gap in employee cybersecurity complaince. In Proceedings of the ICCWS 2019 14th International Conference on Cyber Warfare and Security, Stellenbosch, South Africa, 28 February–1 March 2019; pp. 94–102.
60. Alvarenga, A.; Tanev, G. A cybersecurity risk assessment framework that integrates value-sensitive design. *Technol. Innov. Manag. Rev.* **2017**, *7*, 4. [CrossRef]
61. Baikloy, E.; Praneetpolgrang, P.; Jirawichitchai, N. Development of cyber resilient capability maturity model for cloud computing services. *TEM J.* **2020**, *9*, 915. [CrossRef]
62. Venkatesh, V. Design of Cybersecurity Risk Assessment Tool for Small and Medium Sized Businesses using the NIST Cybersecurity Framework. In Proceedings of the KSU Proceedings on Cybersecurity Education, Research and Practice, 6; 2018. Available online: https://digitalcommons.kennesaw.edu/ccerp/2018/practice/6 (accessed on 24 June 2023).
63. Gourisetti, S.N.G.; Mylrea, M.; Patangia, H. Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. *Future Gener. Comput. Syst.* **2020**, *105*, 410–431. [CrossRef]
64. Kure, H.I.; Islam, S.; Ghazanfar, M.; Raza, A.; Pasha, M. Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system. *Neural Comput. Appl.* **2021**, *34*, 493–514. [CrossRef]
65. Radanliev, P.; Montalvo, R.M.; Cannady, S.; Nicolescu, R.; De Roure, D.; Nurse, J.R.; Huth, M. Cyber Security Framework for the Internet-of-Things in Industry. In *Living in the Internet of Things: Cybersecurity of The IoT-2018*; IET. 4.0; 2019; pp. 1–6. Available online: https://www.preprints.org/manuscript/201903.0111/v1 (accessed on 5 July 2023).
66. Wang, J.; Neil, M.; Fenton, N. A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Comput. Secur.* **2020**, *89*, 101659. [CrossRef]
67. Armenia, S.; Franco, E.F.; Nonino, F.; Spagnoli, E.; Medaglia, C.M. Towards the definition of a dynamic and systemic assessment for cybersecurity risks. *Syst. Res. Behav. Sci.* **2019**, *36*, 404–423. [CrossRef]
68. Lee, I. Cybersecurity: Risk management framework and investment cost analysis. *Bus. Horiz.* **2021**, *64*, 659–671. [CrossRef]
69. Rea-Guaman, A.M.; Mejía, J.; San Feliu, T.; Calvo-Manzano, J.A. AVARCIBER: A framework for assessing cybersecurity risks. *Clust. Comput.* **2020**, *23*, 1827–1843. [CrossRef]
70. Tagarev, T.; Pappalardo, S.M.; Stoianov, N. A Logical Model for Multi-Sector Cyber Risk Management. *Inf. Secur.* **2020**, *47*, 13–26. [CrossRef]
71. Wang, Y.; Wang, Y.; Qin, H.; Ji, H.; Zhang, Y.; Wang, J. A Systematic Risk Assessment Framework of Automotive Cybersecurity. *Automot. Innov.* **2021**, *4*, 253–261. [CrossRef]

72. Setiawan, H.; Putra, F.A.; Pradana, A.R. Design of information security risk management using ISO/IEC 27005 and NIST SP 800-30 revision 1: A case study at communication data applications of XYZ institute. In Proceedings of the 2017 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, Indonesia, 23–24 October 2017; IEEE: Piscataway, NJ, USA; pp. 251–256. [CrossRef]
73. Pandey, S.; Singh, R.K.; Gunasekaran, A.; Kaushik, A. Cyber security risks in globalized supply chains: Conceptual framework. *J. Glob. Oper. Strateg. Sourcing*. **2020**, *13*, 103–128. [CrossRef]