risks

MDPI

Article

Context-Based and Adaptive Cybersecurity Risk Management Framework

Henock Mulugeta Melaku

School of Information Technology and Engineering, Addis Ababa Institute of Technology,
Addis Ababa University, Addis Ababa 1000, Ethiopia; henock.mulugeta@aait.edu.et or
henock.mulugeta@aau.edu.et

Abstract: Currently, organizations are faced with a variety of cyber-threats and are possibly challenged by a wide range of cyber-attacks of varying frequency, complexity, and impact. However, they can do something to prevent, or at least mitigate, these cyber-attacks by first understanding and addressing their common problems regarding cybersecurity culture, developing a cyber-risk management plan, and devising a more proactive and collaborative approach that is suitable according to their organization context. To this end, firstly various enterprise, Information Technology (IT), and cybersecurity risk management frameworks are thoroughly reviewed along with their advantages and limitations. Then, we propose a proactive cybersecurity risk management framework that is simple and dynamic, and that adapts according to the current threat and technology landscapes and organizational context. Finally, performance metrics to evaluate the framework are proposed.

Keywords: cyber-risk; risk assessment; risk impact; likelihood rating; performance metrics

1. Introduction

Cybersecurity risk is the probability of imposing a negative impact on sensitive information and the business process of an organization. Cyber-risks that are most widely occurring include ransomware, phishing, advanced persistent threats (APTs), and insiders (Lee 2021).

Cybersecurity risk management (CRM) is the process of detecting an organization's security threats, discovering security gaps in order to determine the attack scenario, and deciding on how to address the cybersecurity risk. The main goal of cybersecurity risk analysis and assessment is to identify cyber-threats; classify business assets according to their criticality; identify system vulnerabilities; and implement effective security controls to mitigate the identified risk (Kure and Islam 2019; Lee 2020).

In addition, CRM is also a strategic method used to prioritize cyber-threats and risks. As part of the risk management process, organizations should implement a security risk management program to appropriately manage identified cyber-risks and attacks (Lee 2021). This proactive approach supports identifying, analyzing, evaluating, and addressing security attacks and risks based on the possible adverse effect of the cyber-attacks that may be launched on an organization. Under any circumstance, a risk management strategy acknowledges that whatever security controls are implemented, it is impossible for organizations to completely avoid information system (IS) and business process vulnerabilities or prevent security threats. However, by using standard risk management programs, organizations can protect their critical business assets from a wide range of security threats (Uddin et al. 2020).

Most security standards and best practices state that the CRM framework comprises three major and interrelated processes: assessment of the cyber-risk, alleviation of the identified and analyzed risk, and periodic evaluation of the CRM itself (Uddin et al. 2020; Vitunskaite et al. 2019).

check for updates

Citation: Melaku, Henock Mulugeta. 2023. Context-Based and Adaptive Cybersecurity Risk Management Framework. *Risks* 11: 101. https://doi.org/10.3390/risks11060101

Academic Editor: Mogens Steffensen

Received: 7 April 2023
Revised: 15 May 2023
Accepted: 19 May 2023
Published: 31 May 2023

Security risk assessment comprises the identification of cyber-threats and system vulnerabilities, valuation of assets, analysis of the threat impact and its likelihood, determination of the risk, and recommendation of the risk-reduction techniques. At the same time, risk treatment involves choosing and implementing the best risk reduction methods. Moreover, cybersecurity risk management programs should be periodically monitored and evaluated (Frank et al. 2019).

According to the Australian Standard, a CRM framework encompasses developing, applying, monitoring, and periodically evaluating security risk management processes (Frank et al. 2019; Ganin et al. 2020). The CRM framework also comprises security risk management programs, organizational security objectives and goals, security strategy and policy, resources needed to implement security controls, budget, and top management's commitment to deal with security risks. Moreover, it requires an organizational structure, including reporting, communication, accountability, processes, programs, and plans, that is an integral part of the overall organization's risk management strategies and objectives (Frank et al. 2019; Ganin et al. 2020; Tupa et al. 2017). Developing and implementing a CRM framework aims to ensure that risks are identified on time, risks are managed according to the risk appetite defined, resources are effectively used to manage the identified risk, and organizational security workforce and structure are developed. Ultimately, cyber-risk should be appropriately managed in order to achieve strategic security objectives (Tupa et al. 2017; Rostamzadeh et al. 2018).

These days, nations and organizations should protect and secure their critical infrastructures (CIs) using suitable cybersecurity standards and frameworks. Moreover, IS and network infrastructures currently face various security threats from a wide range of sources. Among the different types of cyber-threats, cybercrime and cyber-terrorism have escalated considerably during the last few years, and are well-organized, well-financed, and technically advanced. The old intention of cyber-criminals was quick entry and exit in a given cyberspace. However, the new view is a long-term presence in an IT system to perform malicious activities. As an author (Melaku 2023) found recently in the East Africa region in general, and in Ethiopia in particular, the critical cybersecurity challenges are a lack of cybersecurity governance and risk management frameworks, a lack of incident management plans, and a lack of national and regional legal frameworks related to cybersecurity; a shortage of sufficient cybersecurity professionals, capability, and skills; a lack of security awareness and education program; and a lack of national and international collaboration and cooperation, etc.

Moreover, most organizations depend highly on technological security solutions to protect their IT systems that support the business process. Since the width and depth of the cyber-attack dimension are growing faster than before, technology will provide some solutions for the fastest-growing cyber-attack scenarios. However, cybersecurity is well addressed in addition to technology by designing and implementing a suitable set of governance, risk management, and other frameworks to ensure security and business objectives are met.

Given the above facts, enterprise, IT, and security risk management frameworks are thoroughly reviewed according to their nature, principles, and components. A comparison is made using different framework development metrics and parameters. Finally, a risk management framework is proposed that dynamically changes its risk assessment and analysis processes according to the current cyber-threats and technological landscapes. Moreover, the proposed CRM framework is adaptive and considers the context of an organization.

2. Review of Enterprise, IT, and Cybersecurity Risk Management Frameworks

To explore and manage cybersecurity risks, identifying security attacks and vulnerabilities is paramount to seeing the cyber-risk imposed on an organization. Therefore, appropriate security investment will be made for the risk mitigation decisions. Many cybersecurity risk management frameworks provide standards to identify and mitigate cyber-related risks. The main reasons for having risk management frameworks are that they make it easier for an organization to define the appropriate security-related processes and procedures that are needed to assess, monitor, and mitigate cyber-risks; these frameworks are also used to assess, evaluate, and improve the security status of a company. On the basis of the above useful comprehension, many frameworks, policies, and standards have been developed that help organizations understand their cyber-risk. Some well-known enterprise, IT, and cybersecurity risk management frameworks are presented below.

2.1. Enterprise Risk Management Frameworks

2.1.1. ISO 31000—Risk Management

ISO 31000:2009 delivers values, principles, and risk management guidelines and standards (Tranchard 2018). ISO 31000:2009, Risk Management—"Principles and Guidelines" offers a framework, process, and principles for managing enterprise risk. Any type and size of organization can use the framework. Organizations that use ISO 31000 can accomplish their objectives, increase the probability of identifying threats and opportunities, and enhance the optimal allocation of budget and resources for risk management.

Moreover, it gives complete and actionable steps to deal with internal and external audit programs. In addition, if an organization implements the ISO 31000 framework, it can easily compare its security posture with other recognized standards and best practices.

As shown in Figure 1, ISO 31000:2009 has different risk assessment, evaluation, and treatment phases. Using this framework, organizations can manage their business risk systematically, minimize or accept the risk, identify and remove the root cause of the risk, reduce the likelihood and impact of the risk, contain the risk by following well-versed decisions, and share or transfer the risk to other companies (Tranchard 2018; Rampini et al. 2019).

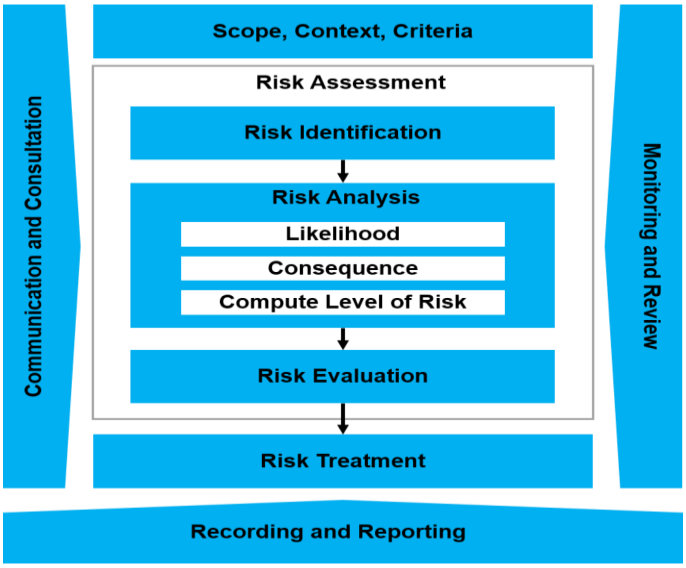


Figure 1. ISO 31000 Enterprise Risk Management Frameworks (ISO31000:2018 Risk Management Process).

2.1.2. Enterprise Risk Management (ERM)—Integrated Framework

This framework was developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) (Rampini et al. 2019; Shad et al. 2019). COSO released this framework in 2004. The framework discusses core principles, processes, and components. It provides guidelines and procedures to manage enterprise risks. It also offers a comprehensive method to manage enterprise risks according to an organization's risk appetite and tolerance. As shown in Figure 2, the framework has five main components to handle enterprise risks: risk assessment, control environment, control activities, monitoring, and information and communication (Shad et al. 2019).

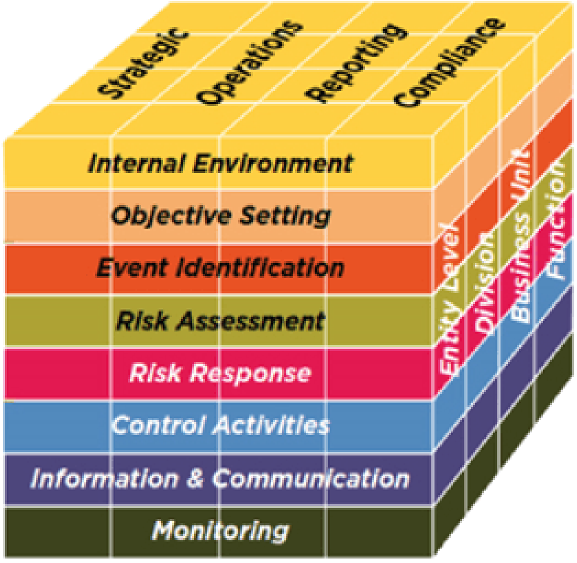


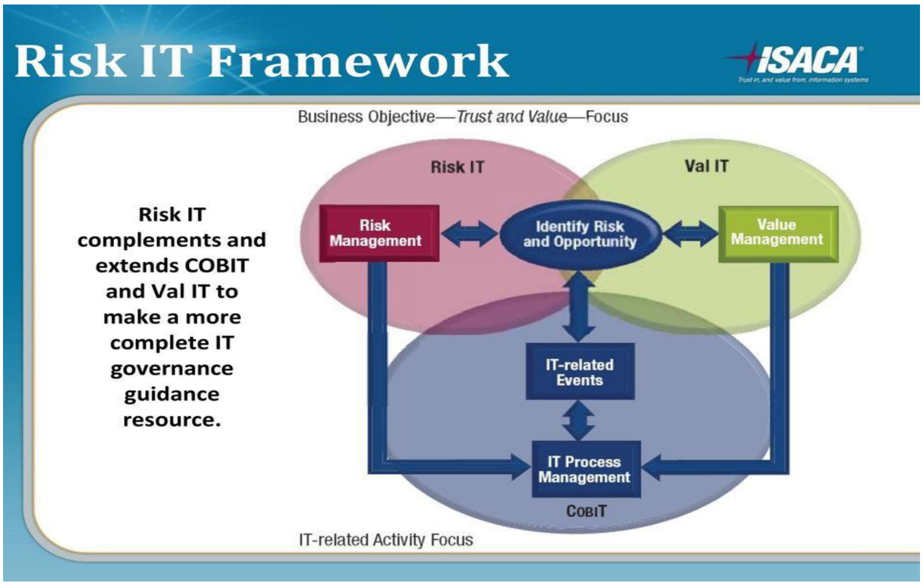
Figure 2. COSO Enterprise Risk Management Framework.

The above two risk management frameworks are mainly used for addressing the issue of general enterprise-level risks. They do not consider IT and security-related risk management frameworks, processes, or programs.

2.2. IT Risk Management Framework

2.2.1. The Risk IT Framework from ISACA—ISACA (Information Systems Audit and Control Association)

The Risk IT Framework is meant to identify and fill the gap between enterprise and IT risk management processes. It also provides guidelines and standards to manage security risks (Kaur and Lashkari 2021). It is an end-to-end approach that makes it suitable to see IT risks holistically. It also includes risk mitigation options. The framework allows organizations to comprehend and manage IT-related risks. Moreover, it builds upon ISACA's most widely used IT risk management frameworks (i.e., COBIT and Val IT). Figure 3 shows a high-level risk management framework proposed from ISACA (Kaur and Lashkari 2021).


Risk IT Framework

Risk IT complements and extends COBIT and Val IT to make a more complete IT governance guidance resource.
ISACA
Trust in, and value from, information systems
Business Objective—Trust and Value—Focus
Risk IT
Val IT
Risk Management
Identify Risk and Opportunity
Value Management
IT-related Events
IT Process Management
COBIT
IT-related Activity Focus

Figure 3. The Risk IT Framework from ISACA.

2.2.2. The IT Infrastructure Library (ITIL) Framework

As shown in Figure 4, the ITIL risk management framework comprises the following core processes: threat identification, vulnerability assessment, probability and impact analysis, determination of the risk, and continuous monitoring of the risk (Wang et al. 2022).

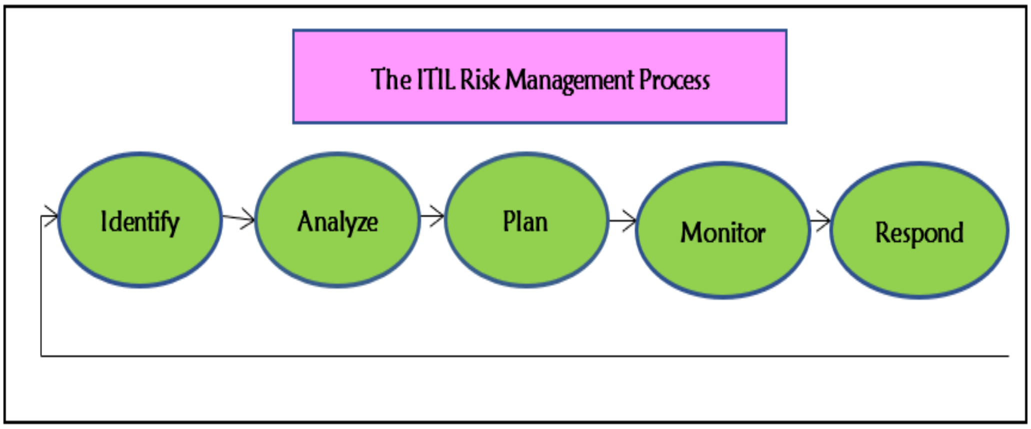


Figure 4. The IT Infrastructure Library (ITIL).

2.2.3. Control Objectives for Information and Related Technology (COBIT 5)

As shown in Figure 5, the IT Governance Institute issued the COBIT 5 framework, which incorporates COBIT 5.0, Risk IT, IT Assurance Framework (ITAF), Val IT 2.0, and Business Model for Information Security (BMIS) (Al-Fatlawi et al. 2021). There are two mechanisms used in COBIT 5. *Risk function*—defines well-structured risk governance and management techniques to effectively manage IT risks. *Risk management*—provides different phases to manage IT risks, such as identifying, analyzing, responding, and reporting risk (Al-Fatlawi et al. 2021).

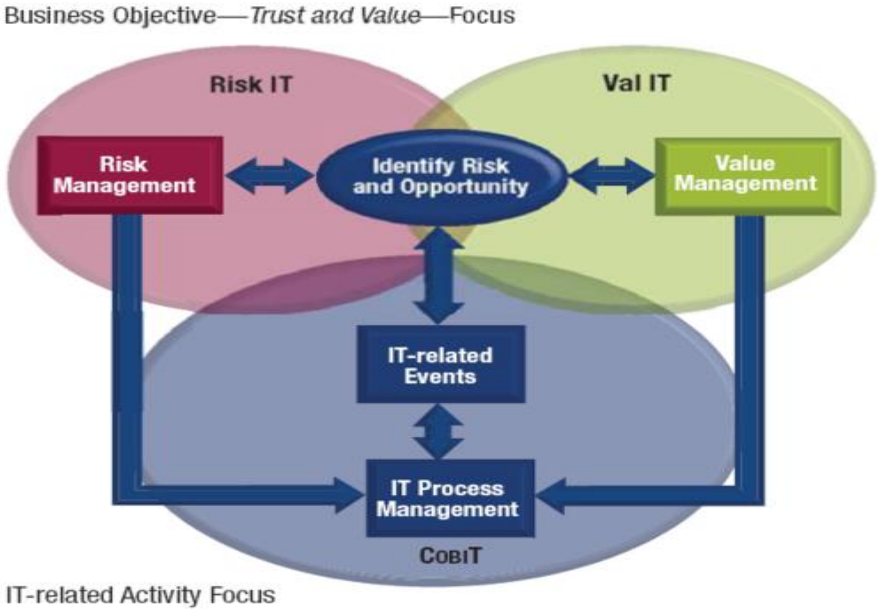

Business Objective—*Trust and Value*—Focus
Risk IT
Val IT
Risk Management
Identify Risk and Opportunity
Value Management
IT-related Events
IT Process Management
COBIT
IT-related Activity Focus

Figure 5. COBIT 5 IT Risk Management Framework.

2.3. *Cybersecurity Risk Management Frameworks (CRMFs)*

Different types of CRMFs have been developed to manage security risks. These CRMFs provide standards and processes to identify, analyze, and mitigate security risks (Lee 2021).

The literature points out that the reason for using cybersecurity RMFs is that they make it easier for organizations to devise suitable processes and procedures that are needed to *assess*, *analyze*, *monitor*, and *mitigate* risks; to define an appropriate set of security processes, policies, and guidelines to address the identified risks; and to measure and enhance the security posture of an organization. In light of the above facts, different cybersecurity risk management frameworks can help an organization evaluate the strength of the security controls they implement. The currently available cybersecurity risk management frameworks tend to have a combination of security and compliance requirements (Goel et al. 2020).

Compliance-based requirements focus on protecting specific data or information. Some of the common compliance-based frameworks are GDPR HIPAA, PCI-DSS, HITRUST, SOC, and FISMA. At the same time, security-focused requirements are based on the organization's environment. NIST and ISO are examples among the many cybersecurity risk management frameworks proposed so far (Sulistyowati et al. 2020).

2.3.1. NIST Cybersecurity Framework

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is one of the most prevalent frameworks in the industry (Gordon et al. 2020). The NIST CSF is a framework that can help companies to manage and mitigate cybersecurity risk in a standard way. As shown in Figure 6, the framework provides five essential and comprehensible functions—identify, protect, detect, respond, and recover—to manage cyber-related risks. It has a technique for mapping between each activity and outcome. NIST is responsible for developing standards, guidelines, and related methods and procedures for delivering adequate cybersecurity.

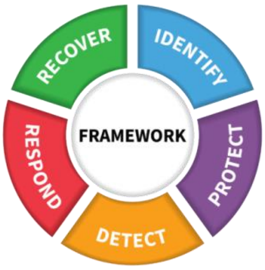


Figure 6. NIST cybersecurity framework.

As shown in Figure 7, risk within the first pillar (Identify), security risk assessment procedures, and guidelines are presented. More specifically, the framework recommends companies take the following steps to identify and analyze risks: identify and document asset vulnerability; acquire up-to-date threat intelligence and identify and document both internal and external threats; identify possible corporate impacts and probabilities of the security risks; make use of threat, vulnerability, probability, and effect to determine the risks; and finally identify and prioritize risk responses.

2.3.2. NIST Cybersecurity Risk Management Framework

NIST SP-800-37 is one of the most commonly used risk management frameworks by organizations. As shown in Figure 7, the NIST Cybersecurity RMF comprises six phases. Each phase comprises different processes to manage cybersecurity risks (McCarthy and Harnett 2014; Almuhammadi and Alsaleh 2017). The NIST RMF provides an all-inclusive, flexible, and repeatable seven-step process to manage security and privacy risks, and relates to a set of NIST standards and guidelines to be applied for risk management programs. In this way, it is possible to meet the requirements of FISMA. FISMA gives direction on the importance of risk management compliance with appropriate laws and regulations, executive orders, directives, etc. The NIST Special Publication 800-37 (Revision 2) is a cybersecurity RMF with a standard process for implementing, monitoring, and evaluating cyber-risks (McCarthy and Harnett 2014). Although the NIST RMF was created by the US Department of Defense (DoD), it provides a worthy reference framework for security and privacy programs that any type and size of organization can use. The NIST RMF comprises seven steps, as shown in Figure 8 below.

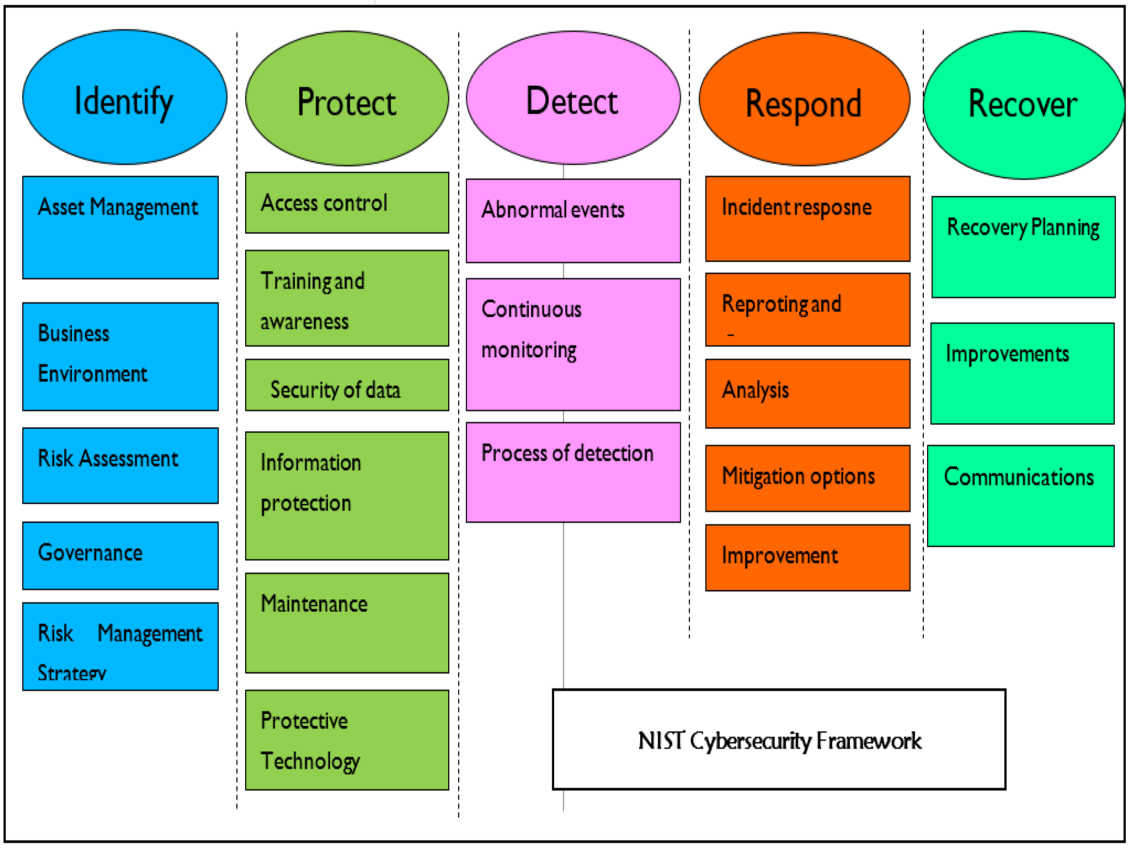


Figure 7. NIST Cybersecurity Framework.

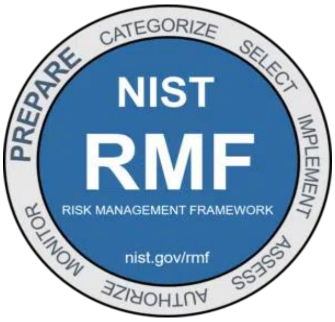


Figure 8. The NIST Cybersecurity risk management framework.

2.3.3. ISO/IEC 27005:2018 Risk Management Framework

This provides a well-defined set of standards and guidelines to systematically manage risks for an organization. It also supports the general concepts that are specified in ISO 27001. ISO 27005 outlines five major pillars that are needed for the management of cybersecurity risk and seven steps that must be followed to perform a risk assessment. These five major pillars are threat identification, vulnerability assessment, risk analysis, risk mitigation, and defining security outcomes (Diamantopoulou et al. 2020). To make it more comprehensive, the ISO 2005 risk management framework comprises five processes: context understanding, analysis of risk, treatment of risk, the suggestion of risk acceptance methods, and monitoring and review of the risk.

2.3.4. OCTAVE

This is a security risk management framework that is composed of the identification, management, and evaluation of security risks. As shown in Figure 9, the OCTAVE framework helps an organization to identify assets, identify security threats and system vulnerabilities, determine the likelihood, analyze the impact, and determine the risk that an organization is willing to accept the risk and pledge constant development activities to mitigate risks (Hom et al. 2020).

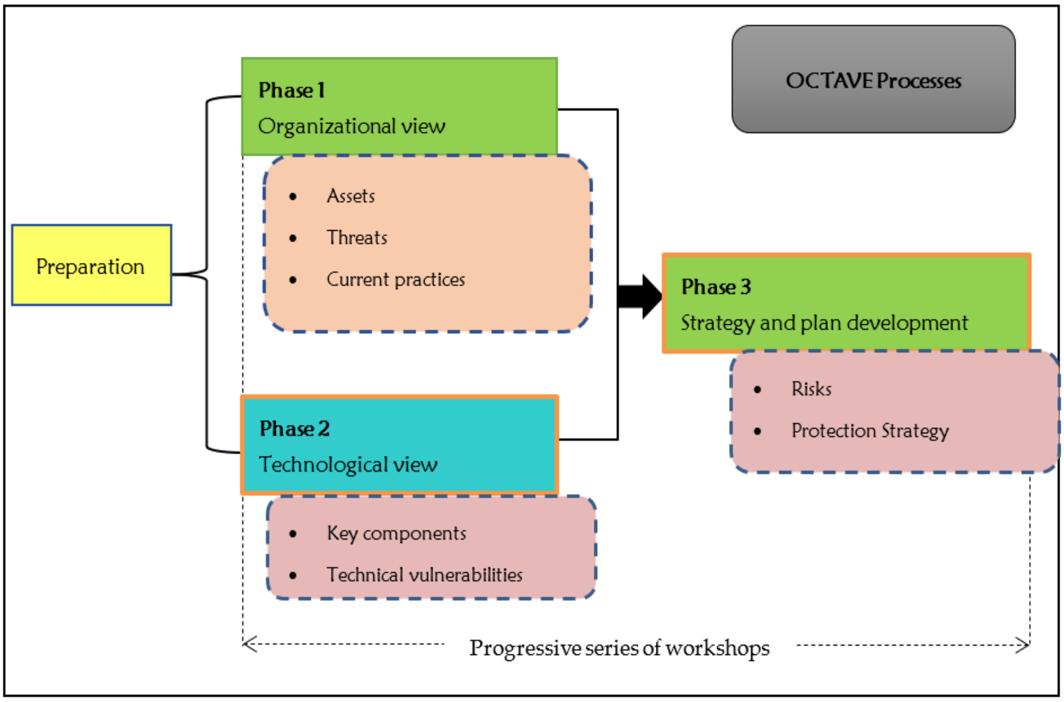


Figure 9. OCTAVE information security risk management framework (Hom et al. 2020).

2.4. Comparison of the Risk Management Frameworks

To compare and analyze the various risk management frameworks presented in Section 2, different parameters, such as risk assessment, risk analysis, risk mitigation, cost and ease of implementation, compatibility, and other parameters, are considered (Tables 1 and 2). According to the analysis made in Table 1, the NIST framework is highly likely to be used by any organization that needs tactical-level risk management due to compatibility and ease of availability and use. It was also developed to be consistent with ISO/IEC standards, allowing for simple integration with pre-existing management systems. It is also freely available and accessible from NIST's website for organizations to implement. It has clear, concise, and controlled instructions that enable it to be used alongside other risk assessment toolkits for a multi-faceted approach. However, some of the limitations of the NIST framework are that, since it is based in the USA, most of the documentation is heavily focused on US regulations and legislation.

Moreover, the implementation support services through NIST are specific to US organizations; hence, sourcing appropriate and localized advice may be difficult. The other drawback of NIST is that it focuses on tactical-level risk assessment. However, it does not consider the strategic- and operational-level risk assessment.

In contrast, ISO 27005 aligns directly with ISO/IEC 27001 for information security management systems and provides a toolset that can be adopted around the specified controls. An organization of any type and size can also implement it. It also provides a basis for organizations to implement their risk management framework; however, it is costlier than the other frameworks. Moreover, it is difficult to understand the implementation details if the user is unfamiliar with ISO/IEC and its security controls.

COSO is complex and hence can be implemented by large and complex organizations. However, it does not incorporate risk assessment and analysis processes.

Unlike NIST, which operates at the tactical level of risk management, OCTAVE is a strategic-level risk management framework that can be applied with minimum cost and can be implemented for any type and size of the organization. It is also very well organized and is freely available. Moreover, OCTAVE addresses all aspects of information security risks from technical, physical, and people perspectives. However, the limitations are that it is complex, and most organizations cannot model the risk. It also follows a qualitative risk management approach.

Table 1. Comparison of different cybersecurity risk management frameworks.

Parameters	NIST	ISO 27005	OCTAVE	COSO	ITIL	COBiT 5	ISO 31000
Risk assessment	√	√	√	√	√	√	√
Risk analysis	√	√	√	×	√	√	√
Risk mitigation	√	√	√	×	√	√	√
Approach	Tactical approach	High-level approach	High-level approach	High-level control capabilities	Holistic approach: customer-focused	Holistic approach	A comprehensive and practice-based approach
Cost	Low cost: free access	High: paid access	Very low cost	Low cost	Higher cost	Free and medium cost	High cost
Implementation	Easy	Easy	Easy	Complex	Complex	Complex	Easy
Compatibility	Any type and size of the organization	Any type and size of the organization	Large organization	Large organization	Any size and type of organization	Simple to complex organizations	Any size and type of organization
Focus area	Tactical-level RM	Holistic RM	Strategic RM	Enterprise RM	End-to-end RM	End-to-end RM	End-to-end RM
Organizational perspective	Allows third-party execution	Assign risk to a third party via outsourcing or insurance	Follows self-directed approach	Allows third-party service provider	Allows third parties such as suppliers	Allows third-party and regulators	None
Technical perspective	√	√	√	√	√	√	×
Assessment team	×	√	√	√	×	×	×
Information gathering	Questionnaires, interviews, document review	Questionnaires, interviews, document review, observation	Workshop based approach	Interviews, workshops, surveys, and benchmarking	Questionnaires, interviews, document review	Questionnaires, interviews, document review	Interviews, workshops, surveys, and benchmarking
Human resources as an asset	×	√	√	√	√	√	√
Software tools used	√	√	√	√	×	√	√

Table 2. ISRM phases for different risk management frameworks (table is adopted from Faris et al. 2014).

ISRM Phases	ISRM Output	NIST	ISO 27005	OCTAVE
Characterization of IS and business process.	List of company's assets that require security and defining the risk appetite and acceptance level	System characterization	Critical asset identification and categorization	Determination of the currently implemented security practice, System characterization and context understanding
Identification of cyber-threat and vulnerability	Identification of cyber-attacks and security vulnerabilities that may affect the already classified assets	List of identified threat intelligence, system vulnerability, and security control analysis	Threat and system vulnerability identification	Threat identification, system vulnerability identification

Table 2. *Cont.*

ISRM Phases	ISRM Output	NIST	ISO 27005	OCTAVE
Analysis and definition of risks	Likelihood determination, impact analysis, and risk analysis and determination	Determination and rating of probability, impact analysis, and determination of risk	Potential impact analysis, likelihood determination, and risk identification	Impact analysis, probability, and risk determination
Analysis of security controls	Cost-benefit analysis and recommendation of various security controls to reduce the risk to an acceptable level	Analysis and recommendation of security controls	Analysis of risks and recommendation of risk reduction techniques	Detail analysis of risk and recommendation of security controls
Evaluation and implementation of security controls	Evaluation, recommendation, and implementation of security controls	Security control recommendation, cost-benefit analysis of security controls, implementation and evaluation of security controls	Recommendation of risk treatment/mitigation methods (reduction, avoidance, transfer, or retention)	Cost-benefit analysis, evaluation, implementation, and planning for the recommended security controls to protect the most critical assets

3. Related Works

The authors of a previous study (Goel et al. 2020) proposed a risk assessment framework that helps top management to make a strategic decision based on the outcome of security risk. The framework is called PRISM and can be used by an organization's top management to manage risk and operationalize strategically at tactical and operational levels. The authors claimed that the proposed framework could help companies to manage cybersecurity risks using the most tailored risk management and assessment method. However, the proposed framework focuses on strategic-level risk management. The tactical- and operational-level risk assessment was not considered.

The authors of another study (Pandey et al. 2020) proposed a conceptual risk management framework for supply chain management. The authors thoroughly examined the cybersecurity risks likely to happen to the supply chain process. It is noted in the paper that security risk has a large impact on the performance of the global supply chain process. Moreover, the authors investigated the cyber-physical system threats and vulnerabilities that influence the supply chain system. The proposed framework identifies various cyber-risk and attacks in the global supply chain, which are then categorized as demand, supply, and operational risks. Finally, they propose a framework to minimize the supply chain attack surface, system vulnerabilities, and threats, and provide risk mitigation strategies. However, the framework is tailored to work for supply chain attacks.

Lee (2020) reviewed Internet of Things (IoT) technologies and various cybersecurity risk management frameworks. Then, the author proposed a risk management framework composed of four layers tailored to be applied to IoT systems. The paper also proposed a linear-programming-based financial resource allocation for different IoT projects. The limitation of the paper is the developed framework only works for IoT networks. It does not consider other network infrastructures such as the cloud, software-defined networks, or traditional network types.

The authors Kure and Islam (2019) proposed a risk management framework focused on critical infrastructure assets (CIs). Additionally, they proposed a method that can systematically identify and analyze core assets in the CIs. The proposed framework can identify threats and vulnerabilities that could be exercised by threat sources for critical assets. Risk analysis techniques are also proposed as an integral part of the framework. They used a running smart power grid system as a case study. Their research output confirmed that the framework works well by identifying more critical assets along with their security holes and the cascading effect on the other business process. However, as a limitation, the framework mainly focuses on critical assets and works only for critical infrastructure. It does not consider IS and business process assets in a given CI.

Moreover, the focus of the paper is on the identification of threats and vulnerability rating. The other processes of risk assessment, such as impact analysis, likelihood determination, and thorough risk analysis techniques, are not proposed. Moreover, security control recommendations and risk mitigation options are not considered.

The authors of another study (Ganin et al. 2020) proposed a decision-based risk management framework. The focus of the proposed framework is to fill the gap that was reviewed and identified in other frameworks. The authors reviewed probabilistic and risk-based decision approaches to cyberspace. They concluded that existing approaches did not address the core components of risk assessment processes, such as threat and vulnerability identification and consequence analysis. The proposed framework fills the gap between risk management and assessment processes. However, evaluation methods using key performance indicators (KPIs) and validation of the proposed framework are not incorporated.

Research gap: Though different risk assessment and management frameworks have been developed, the most relevant frameworks are reviewed and presented. Existing risk management frameworks are too complex to be implemented by organizations. Some of the frameworks are mainly designed to be implemented for some types of application scenarios and network systems, while others are focused on some parts of the risk assessment phases, such as asset identification and valuation. The other frameworks focused on vulnerability assessment and threat identification techniques. Other frameworks focused on risk assessment at the strategic level, ignoring the tactical and operational levels. Moreover, almost all the proposed frameworks by different scholars lack the integration of well-known frameworks such as NIST and ISO with their proposed framework.

4. Research Method

The design science research process (DSRP) model was used. In this research context, the DSRP research model comprises problem identification and motivation, objective identification for the solution, design and development of the CRM framework, demonstration of the framework, and finally, evaluation and validation of the developed framework. Each phase is presented below.

Problem Identification and Motivation: To identify the problems or gaps and to find the motivational factors to conduct this study, the researchers reviewed different literature, existing documentation, standards, best practices, and systems that are currently used by various nations and organizations to secure their network infrastructures. However, most organizations (both public and private sectors) are primarily relying on technological solutions to protect and secure their information and networking infrastructure. Moreover, the technology solutions are not optimally and efficiently implemented and utilized, which leads to more vulnerability to various types of cyber-attacks and threats.

The objective of a solution: This research study aims to design a security risk management framework for organizations to protect and secure their information and technology systems.

Design and development: This activity involves designing and developing various cybersecurity frameworks. The researcher designed and developed a security risk management framework.

Demonstration: This activity presents the use of the artifact (in this research, the framework) to solve the identified problem. The essential requirement that is required for demonstration is to gain enough knowledge about how the framework works or how to use the framework to solve the stated security-related problem. To this end, the research output will be demonstrated in selected sectors.

Evaluation: This activity is all about measuring how well the developed framework solves the existing problem. This is accomplished by associating the stated research objectives with the observed result of the framework regarding the identified problem.

To this end, the research output was evaluated and tested using different performance indicators and evaluation scenarios.

The limitation of this research is that the proposed framework is not validated on selected sectors.

5. Proposed Cybersecurity Risk Management Framework

Firstly, we developed a guideline for designing a cybersecurity risk management framework. To develop a security risk management framework, one has to consider the following issues:

- Recognize the security posture and landscape of an organization: One has to thoroughly investigate and understand the security culture, posture, and landscape of the organization.
- Create a cybersecurity risk management team: It is essential to create a cybersecurity risk management team to address the constantly evolving security threats and to assess and analyze security risks periodically.
- Responsibility assignment: As a company, all employees should be aware of the importance of securing the IT system and business processes and the potential security risk that may damage and disrupt the core business processes. Accordingly, a mechanism should be designed to give every employee roles and responsibilities to mitigate the cyber-risk.
- Train employees on cybersecurity risks: This is used to create a security-aware workforce across the organization. Cybersecurity risk management training, education, and awareness (SETA program) should be prepared to ensure that employees are conversant about how to mitigate the identified security risks so that risk will be mitigated across the organization in comprehensive and holistic approaches.
- Develop and Implement cybersecurity policy: Security policies should be developed and implemented upon completion of risk assessment. This policy will provide every employee with a clear understanding of the security.
- Implement a standard CRMF: Thoroughly investigate and analyze the currently available CRMFs, standards, and best practices and choose one or more to implement. The most frequently used cybersecurity frameworks are ISO/IEC and NIST frameworks. However, according to the nation’s and organizations’ context, values, and other factors, we have developed a context-based cybersecurity risk management framework adaptable to the dynamic threat and technological landscape.
- Develop a risk assessment method: Through a well-versed security risk assessment program, the company can see the security risk imposed on it that may affect the core business process and IT systems, and develop viable risk reduction or mitigation techniques.
- Create and maintain an incident management and business continuity plan: Any cyber-incidents that may not be handled in a risk management program should be reactively handled using a well-prepared incident handling plan. If the incident bypasses the threshold value, it will be escalated and considered a disaster. Therefore, disaster recovery procedures will be implemented. While the main business site recovers from the disaster, normal business should be resumed from an alternate site using a business continuity plan. To perform all of these steps, there is a need to develop these three plans.

The proposed cybersecurity risk management framework presents a standardized and well-documented methodology for the following: (1) conducting a cyber-risk assessment, which evaluates business priorities and identifies gaps in cybersecurity controls; (2) performing risk analysis on the existing security controls that are implemented; (3) prioritizing future cybersecurity investment based on the output of risk analysis; (4) performing security strategies by implementing security controls; and (5) measuring and scoring cybersecurity programs, plans, and processes along the way.

Implementing the proposed cybersecurity RMF helps business organizations to perform activities such as properly identifying cybersecurity risks, clearly comprehending where the organization is more vulnerable, recognizing the potential damage of the identified cyber-risks, and defining a security strategy and policy for protecting the company against cyber-threats. The aim of these activities is to know how to minimize the impact of cyber-attack, to overcome the identified risks using various risk mitigation options, to make sure that the investments in security controls are efficient and effective, and finally to give priority to the security controls and budget based on security risks.

Figure 10 shows the proposed cybersecurity risk management framework. It comprises four major components: *cybersecurity risk assessment*, *mitigation*, *risk management program*, *and process evaluation*.

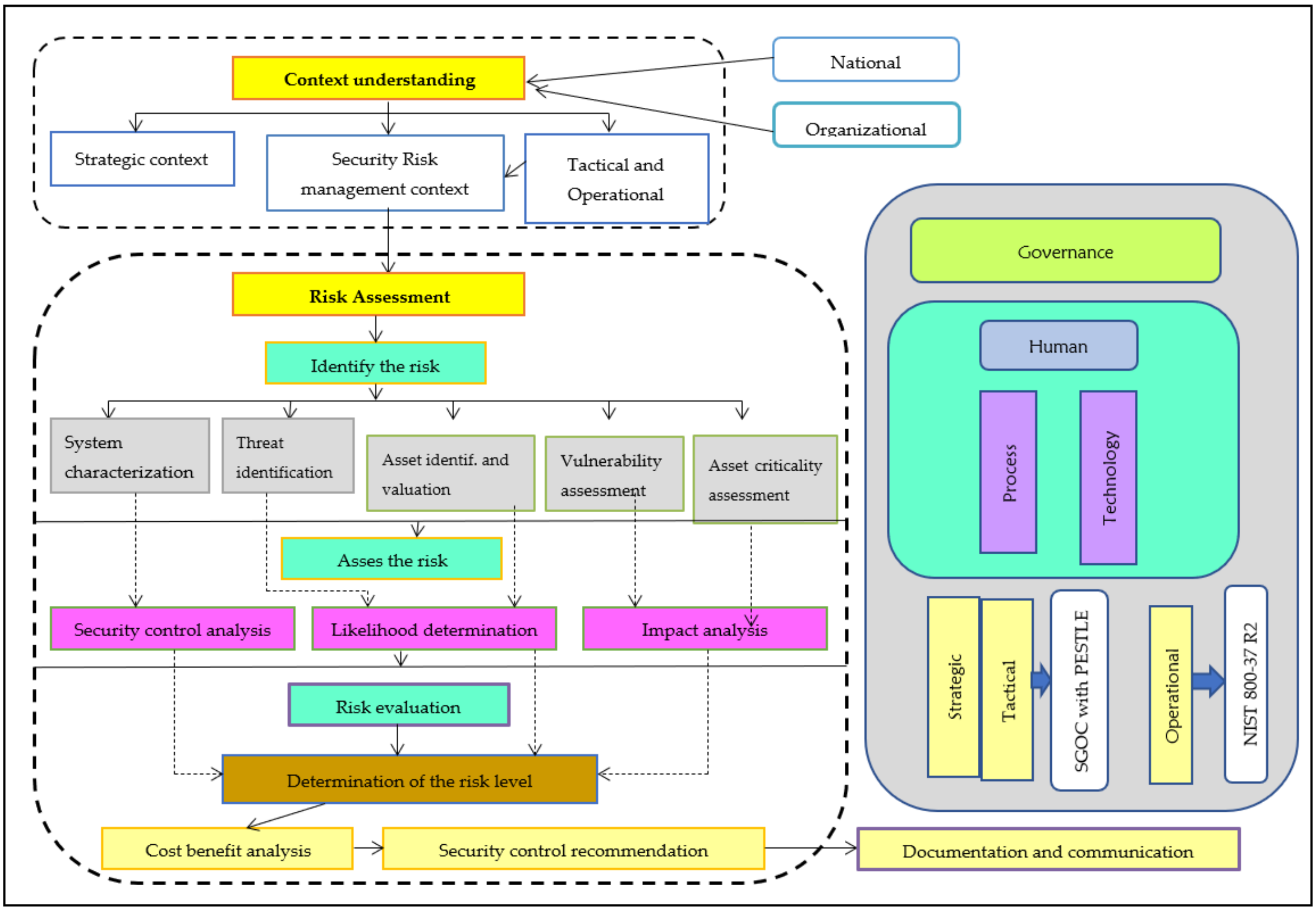


Figure 10. Proposed cybersecurity risk management framework.

Context Understanding: According to ISO 31000, top management should understand the organization's internal and external context and factors that may affect its IT system and business processes (Spross et al. 2022). By understanding the organization's context benefits, the company properly aligns its security risk management strategy with the overall risk appetite and risk tolerance to obtain a competitive advantage without compromising business continuity. In general, understanding organizational context will offer a valuable understanding of the critical IT systems and business processes that are likely to be attacked, the potential cyber-criminals who are interested in that organization, and where the system vulnerability and attack surfaces are that the threat actors will likely use.

Interested parties should also be considered to understand the context of the organization. An interested party is a stakeholder, i.e., an individual or group affected by the organization's information security activities. Understanding the requirements and reactions of stakeholders is a must before a security risk assessment is performed. Some of the interested parties that are considered can be employees, owners and shareholders, government agencies and regulators, clients, suppliers, and partners. The most important thing is understanding what all interested parties want from the business and how to satisfy their requirements through the security program.

Determine risk appetite or tolerance: Risk appetite or tolerance is the amount of cyber-risk a given organization is prepared to accept to achieve its business goals and objectives without problems (Chen et al. 2022). Defining risk tolerance or appetite allows an organization's top management to clearly define the level of risk an organization is willing to accept.

Cybersecurity risk assessment: A security risk assessment describes the methods used to identify, analyze, and prioritize security-related risks of an IT system that is meant to support the business operation (Kandasamy et al. 2020). Without performing a risk assessment, developing appropriate security policies to protect and secure the company's valuable assets is impossible. Cybersecurity risk assessment should be integral to an organization's risk management process. The first step of risk assessment is to identify the security risk, which is composed of the following activities:

A. System characterization: This aims to define the scope and boundary of the IT system that supports the business process (Al-Karaki et al. 2022). Moreover, it provides IT system-related material such as hardware, software, information, system connectivity, interfaces, network diagram, system security architecture, flow of information, technical and management security controls, and operational and physical security controls. All this system-related information can be collected using questionnaires, on-site interviews, document reviews, and security scanning tools. Performing the above activities will give the following outputs: characterization of the IT system, the definition of the scope and boundary, and a good picture of the overall IT system and business environment.

B. Threat identification: A threat can be defined as the likelihood of a given threat actor penetrating a given IT system using a threat vector (Akinrolabu et al. 2019). When defining the probability of a threat or cyber-attack, one must determine the potential sources, security vulnerabilities, and existing security controls. In this step, threat source identification and producing threat statements are paramount for the subsequent phases of risk assessment. The most common threat sources are natural, man-made, and environmental. This step will produce a compiled threat statement containing a potential list of threat sources that are likely to penetrate using the system attack surface and vulnerabilities.

C. Asset identification and valuation: An asset is defined as an item of value to the achievement of the organizational mission/business objectives (CNSSI 4009-2015). Assets may be tangible physical assets such as hardware, software, firmware, computing platform, network device, or technological components. They can also be intangible assets such as human assets, information, software, copyrights, and patents (NIST SP 800-160 Vol. 2 Rev. 1). In general, identifying organizational assets can be achieved through two steps, namely, defining and understanding the organization's primary operations and processes, and identifying the company's critical infrastructure such as critical assets, critical IT systems and data, and security systems.

Once assets are identified, the value should be given to the most critical assets on which the business has relied. One has to put a value on the organizational assets. The most widely used asset valuation techniques are quantitative and qualitative assessments.

Quantitative assessment is described in terms of monetary value (Aven 2015; Ni et al. 2022; Woods and Böhme 2021). It assigns a cost value to the identified assets. To perform a quantitative risk assessment, all phases of the risk assessment processes, such as threat frequency identification, asset valuation, impact analysis, security control efficiency, and costs, impact, and likelihood, should be quantified.

The calculation to determine the cost is presented as:

1. Single Loss Expectancy (SLE)—This calculates the loss of single asset value (AV) and its expectancies using exposure factor (EF). It is calculated as follows:

$$\text{SLE} = \text{AV} \times \text{EF} \tag{1}$$

2. Annual Rate of Occurrence (ARO)—This defines the probability of occurrence of a threat per specified time. It is meant to describe how many times a specific threat happens per year.
3. Annual Loss Expectancy (ALE)—This is meant to determine the level of the risk along with the impact and loss of assets. It is calculated as:

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

As an example, a sample quantitative asset valuation is presented in Table 3.

Table 3. Quantitative asset valuation example.

Asset	Security Risk	Asset Value	Exposure Factor	SLE	Annualized Frequency	ALE
Database	Hacked	USD 250,000	0.17	USD 42,500	0.5	USD 21,250
Webserver	DDoS	USD 300,000	0.5	USD 150,000	0.25	USD 37,500

Qualitative assessment does not assign a dollar value to the assets; rather, it is mainly focused on the scenario-based assumption of the values of each asset (Aven 2015). In contrast, quantitative asset valuation is challenging to accomplish since it is hard to estimate the costs of some assets in terms of monetary value. Therefore, qualitative risk analysis can be expressed in terms of systematically defined rates such as low, medium, and high. These kinds of qualifying technique are given in NIST 800-26.

D. Vulnerability assessment: Vulnerability is the security hole or weakness in protection mechanisms (Uddin et al. 2020). As an organization, the IT system's security vulnerability and business processes should be identified, and a more elaborate vulnerability assessment based on probability is presented in the literature (Gordon and Loeb 2002). The main aim is to develop a list of system vulnerabilities that security threats can use. There are a large number of mechanisms to get around the security vulnerability of the system environment. Some of them are the use of a security requirement checklist, the security testing report, standard vulnerability causes, the result of a system certification test and evaluation, vendors' web pages and the Internet, previous security risk assessment reports, vulnerability lists such as the NIST I-CAT vulnerability database, audit reports, penetration testing, and security testing and evaluation. In general, the result of the vulnerability identification step is to produce documented system vulnerabilities that attackers might exploit.

E. Security control analysis: Currently implemented security controls should be analyzed to ensure that security threat sources cannot exploit the system using security vulnerabilities (Kandasamy et al. 2020). An organization can implement various types of security controls. Some of these are cryptography, intrusion detection systems (IDSs), access control, authentication mechanisms, security policy and procedures, and security governance and management.

F. Likelihood determination means the probability that a cyber-attacker might launch security attacks using system vulnerabilities (Sheehan et al. 2019; Aven 2015). When likelihood is determined, the following factors must be considered: the attacker's motivation and capability, system vulnerability, and the implemented security controls. Likelihood rating can be expressed as low, medium, or high.

G. Impact analysis: This step determines the impact of a given threat source being actualized or penetrating using a system vulnerability to damage the IT system and business operation. Before analyzing the impact, it is essential to determine system and information criticality and sensitivity. This information can be found by performing a business impact analysis and asset criticality assessment. The potential impact can be expressed using the security triad: availability, integrity, and confidentiality. The magnitude of the impact can be determined using quantitative or qualitative techniques such as high, medium, or low (Sheehan et al. 2019; Kandasamy et al. 2020).

H. Determination of the security risk: In this step, the security risk level can be well determined using three parameters (Mazzoccoli and Naldi 2020):

- The likelihood of a given security threat that may use system vulnerability;
- The degree of the impact of the attacks that exploited a system vulnerability;
- The effectiveness of the currently implemented security controls.

Using the above three important parameters, it is possible to determine the security risk level using the risk scale and risk-level matrix that is shown in Table 4.

Table 4. Risk analysis matrix.

	Impact			
Likelihood		**Low**	**Medium**	**High**
	Low	*Low*	*Low*	*Low*
	Medium	*Low*	*Medium*	*Medium*
	High	*Low*	*Medium*	*High*

I. Security control recommendation: This can be found from the output of risk assessment results and will be a valuable input into the risk mitigation options. The recommended security controls are evaluated, prioritized, and implemented in this phase. Cost–benefit analysis of security controls shall be performed to determine which security controls are best suitable. The output of this phase is to recommend security controls to mitigate the security risk that was assessed in the previous risk assessment steps.

J. Documentation: Upon completion of assessing the cyber-risk, such as identifying the security threat source and system vulnerability, cyber-risk is clearly and completely determined, and various security controls are recommended according to the amount of risk identified; the final result should be documented and provided for the top management. A cyber-risk assessment report is a management report that will be provided to top management and business owners to make policy decisions and allocate resources, budget, and other related issues.

6. Cybersecurity Risk Mitigation Options

Risk treatment/mitigation is a method used by the top management of an organization to reduce the already assessed cyber-risk (Mazzoccoli and Naldi 2020). Mitigation of the identified risk can be addressed using the methods shown in Figure 11.

Risk assumption: This involves agreeing to take the cyber-risk and carry on the operation of the IT system that supports the business operation or to implement recommended security controls that are meant to minimize the cyber-risk to an acceptable risk level known as the risk appetite of the enterprise.

Risk avoidance: This is meant to avoid cyber-risk by removing the risk causes or sources, such as by giving up some of the system functionality and shutting down the system when the risk is identified.

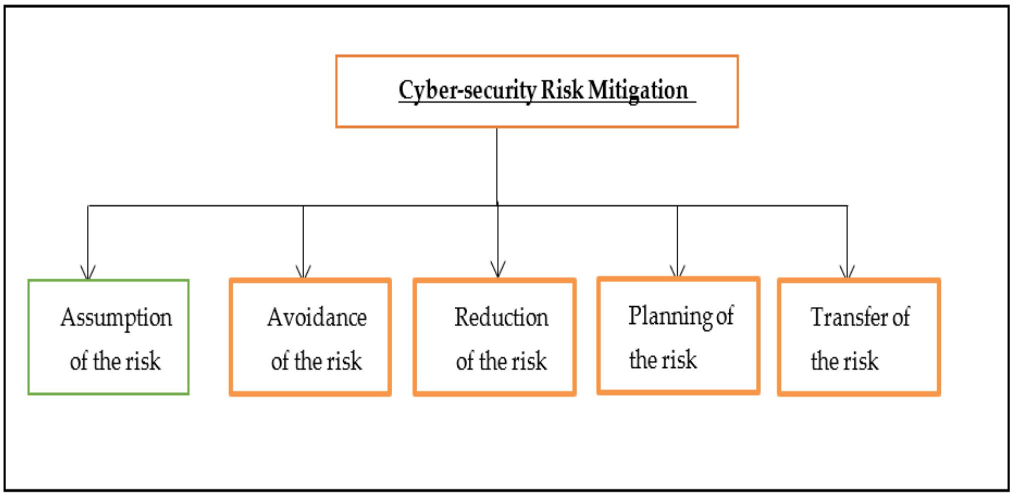


Figure 11. Risk mitigation options.

Risk limitation: By implementing security controls such as using preventive, supportive, or detective techniques, limit the potential impact of threat sources that may exploit system vulnerability.

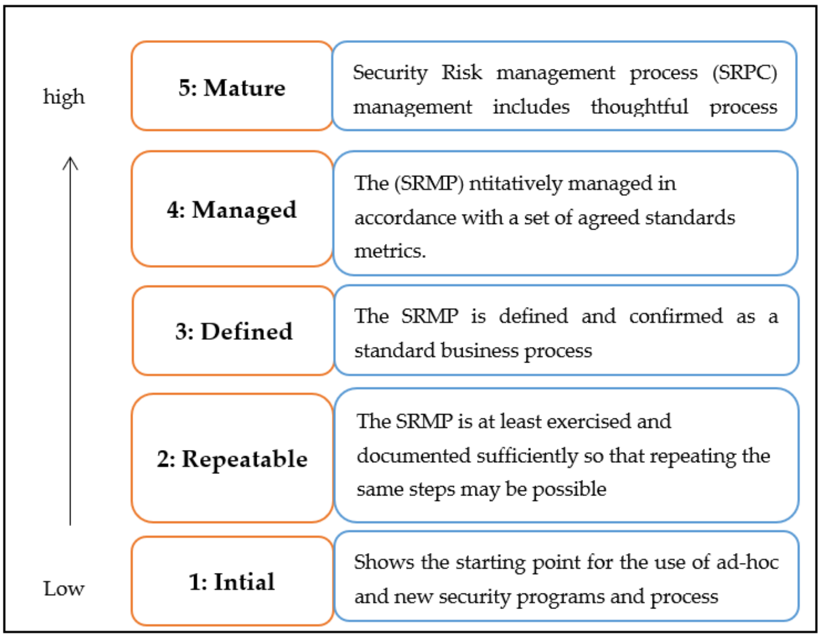
Risk planning is used to manage risks using risk mitigation plans such as IRP, BCP, and DRP.

Risk transfer: To transfer the risk to another third party to gain compensation for losing the company's assets due to a cyber-attack. Some risk transfer techniques are shifting the risk to other assets and processes, or other organizations, purchasing cyber-insurance, and outsourcing to other organizations.

7. Measuring the Cybersecurity Risk Management Framework

Measuring the benefits that the risk management framework brings to an organization is a complex and challenging task. To mitigate this challenge, the measurement of the risk management framework performance should be seen from different perspectives and needs to consider multiple factors. To this end, we propose a mechanism to measure the risk management framework and programs. The measurement can be divided into three different categories:

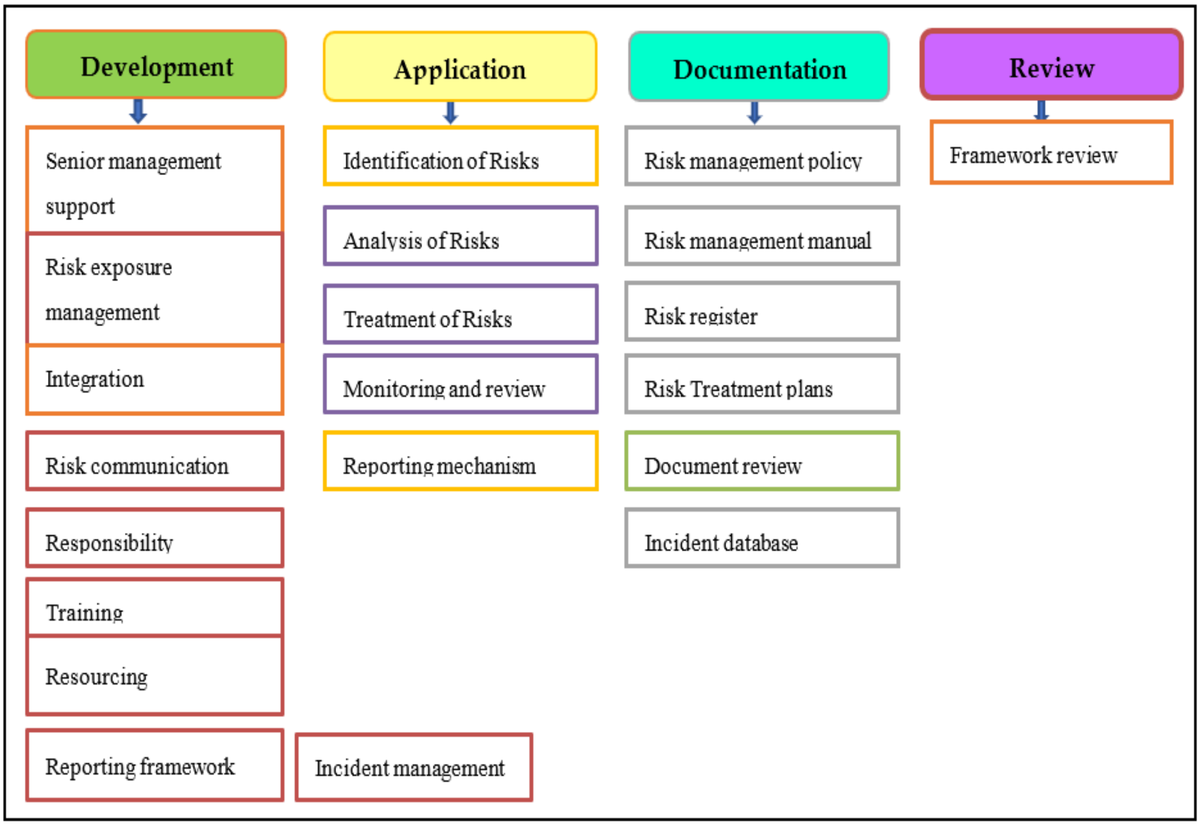
Capability Maturity Assessment Model: This measures the security program's effectiveness within an organization using industry standards and best practices. As noted in Section 4, one of the first steps to establish a security risk management framework for any type and size of organization is to evaluate the existing risk management program, process, and systems. In light of the above fact, the most efficient mechanism of understanding the current trend and status of the security program and process within a company is by performing and conducting a security capability maturity assessment. The risk management program and process should follow the capability maturity model with five levels, as shown in Figure 12 below.



5: Mature	Security Risk management process (SRPC) management includes thoughtful process
4: Managed	The (SRMP) ntitatively managed in accordance with a set of agreed standards metrics.
3: Defined	The SRMP is defined and confirmed as a standard business process
2: Repeatable	The SRMP is at least exercised and documented sufficiently so that repeating the same steps may be possible
1: Intial	Shows the starting point for the use of ad-hoc and new security programs and process

Figure 12. Capability maturity assessment model.

The maturity assessment models can have the subcategories shown in Figure 13.



Development
- Senior management support
- Risk exposure management
- Integration
- Risk communication
- Responsibility
- Training
- Resourcing
- Reporting framework

Application
- Identification of Risks
- Analysis of Risks
- Treatment of Risks
- Monitoring and review
- Reporting mechanism
- Incident management

Documentation
- Risk management policy
- Risk management manual
- Risk register
- Risk Treatment plans
- Document review
- Incident database

Review
- Framework review

Figure 13. Risk assessment checklists.

Conformance measures whether the organization conforms to its security risk management policy directives. In addition to the maturity assessment techniques, risk management programs should go through conformance auditing. The primary function of conformance auditing is to ensure that the basic security requirements presented in the organization risk management policy are followed. Moreover, the company can also compare itself with other best practices and standards.

Value adds: This measures the extent to which the risk management program contributes to better accomplishing the company's security objectives and outcomes.

8. Discussion, Comparison, and Research Implication

The main aim of proposing a new cybersecurity risk management framework is to review the existing CRMFs, make a comparison, and analyze their possible gaps, overlaps, and limitations. This is followed by proposing an adaptive, holistic, and dynamic conceptual risk management framework that fills the gaps and limitations and is observed from the analysis process. Moreover, we have incorporated and used knowledge from the literature in the domain, white papers, and other publicly available resources to enrich the proposed framework.

The proposed framework can be used for strategic, tactical, and operational risk management and assessment. However, regarding the other frameworks, some are used at the strategic level, while others are either tactical or operational. Most of the existing frameworks are too complex to be implemented by organizations. However, the proposed framework is simple to implement by an organization that has a very low-security posture. In almost all of the existing frameworks, there is an implementation cost. However, the proposed framework can be used without payment as it is mainly focused on developing countries. The other feature of the proposed framework is that it primarily focuses on understanding the context of an organization, even at the national level, including internal and external, and the various stakeholders before a security risk assessment is made. The existing frameworks focus on the risk assessment part. Moreover, when the organization's maturity is enhanced, in the proposed framework, there is room for the integration of other frameworks, such as NIST at the operational level and SGOC with PESTLE at the tactical and strategic levels. Additionally, in the proposed framework, risk assessment is mainly performed from three security pillar perspectives: technology, human, and process.

The research output will be of paramount importance to nations and organizations in several ways. As discussed, cybersecurity that can be achieved through technical means alone provides a minimal protection scheme. Therefore, it should be supported by appropriate governance, management, and procedures. To this end, organizations, including CIs, can use the framework to protect their information system and business processes. Unless a security risk assessment is performed, a company cannot develop a security policy, implement security controls, and design security programs and plans as part of the proposed frameworks.

Since cybersecurity needs to be considered as a risk management issue like other IT and enterprise risks, including huge complex financial and other critical risks, it should be treated and dealt with in the organization's context. Moreover, since cyber-risk should be addressed from multiple perspectives and levels, it requires an adaptive protection strategy. Finally, cyber-risk needs a collaborative and holistic approach. The proposed framework is incorporated as part of its components and processes to achieve the aforementioned requirements of cyber-risk, such as context understanding, addressed from multiple levels, and the need for a holistic and collaborative approach. To this end, if organizations implement the proposed framework by following the above principles, they will be more resilient to cyber-attacks and effectively use their security budget and resources. Finally, suppose an organization implements the proposed framework. In that case, they will obtain the following benefits: top management will have a clear understanding of their cyber-risk so that an appropriate security policy, strategic decisions, and effective resources will be developed and allocated; they will know their significant cyber-threats to act accordingly; they will be able to mitigate the identified risk using recommended mitigation options; they will also be able to develop a risk treatment plan to implement the appropriate security controls; and they will be better able to reduce cyber-incidents and their impacts.

9. Conclusions

In this research study, well-known risk management frameworks from enterprise, IT, and cybersecurity perspectives are reviewed and compared thoroughly using different comparison metrics. Moreover, the most relevant recently published papers regarding the problem area are presented along with the research gap. Then, a cybersecurity risk management framework that is flexible, adaptive, and dynamic, and that changes according to the current technological and threat landscape, is proposed. Performance metrics to evaluate the framework are also proposed and discussed. The framework's research implication and adoption are presented along with the limitation of traditional security strategy and solutions. The proposed framework can be used at strategic, tactical, and operational risk management and assessment levels. Most of the existing frameworks are too complex to be implemented by organizations. However, the proposed framework is simple to implement by an organization having a very low-security posture. The other feature of the proposed framework is that it mainly focuses on clearly understanding an organization's context, even at the national level, including internal and external levels, and various stakeholders before a security risk assessment is made. Moreover, when the organization's maturity is enhanced, in the proposed framework, there is room for the integration of other frameworks, such as NIST at the operational level and SGOC with PESTLE at the tactical and strategic levels. Finally, in the proposed framework, risk assessment is mainly performed from three security pillar perspectives: technology, human, and process. The performance of the proposed framework can be measured using three techniques: the capability maturity model, conformance, and value add techniques.

Funding: This research is funded by Addis Ababa University with grant number AAU/TR/217/20.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: We thank and acknowledge Addis Ababa University (AAU) for granting funds to conduct this research study. We would also like to express our deepest gratitude to many governmental and private organizations that opened their doors for this research activity. Parts of this research were undertaken with Information Network Security Administration (INSA) and Artificial Intelligence (AI) staff members (MSc and PhD students in cybersecurity). Therefore, very special thanks go to INSA. The authors also thank staff members, data collectors, literature reviewers, and many others who have directly contributed to this research study's success. A very special thanks goes out to Worku Gachena (Director, Ethiopian Artificial Intelligence Institute) for the valuable financial support he offered to the output of this research. Finally, I would like to thank Sileshie Demesie for the proof reading of the manuscript.

Conflicts of Interest: The author declares no conflict of interest.

References

Akinrolabu, Olusola, Jason R. C. Nurse, Andrew Martin, and Steve New. 2019. Cyber risk assessment in cloud provider environments: Current models and future needs. *Computers & Security* 87: 101600.

Al-Fatlawi, Qayssar Ali, Dawood Salman Al Farttoosi, and Akeel Hamza Almagtome. 2021. Accounting information security and it governance under cobit 5 framework: A case study. *Webology* 18: 294–310. [CrossRef]

Al-Karaki, Jamal N., Amjad Gawanmeh, and Sanaa El-Yassami. 2022. GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking. *Journal of King Saud University-Computer and Information Sciences* 34: 3079–95. [CrossRef]

Almuhammadi, Sultan, and Majeed Alsaleh. 2017. Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT)* 7: 51–62.

Aven, Terje. 2015. *Risk Analysis*. Hoboken: John Wiley & Sons.

Chen, Zhen-Song, Xuan Zhang, Rosa M. Rodríguez, Witold Pedrycz, Luis Martínez, and Miroslaw J. Skibniewski. 2022. Expertise-structure and risk-appetite-integrated two-tiered collective opinion generation framework for large-scale group decision making. *IEEE Transactions on Fuzzy Systems* 30: 5496–510. [CrossRef]

Diamantopoulou, Vasiliki, Aggeliki Tsohou, and Maria Karyda. 2020. From ISO/IEC27001: 2013 and ISO/IEC27002: 2013 to GDPR compliance controls. *Information & Computer Security* 28: 645–62.

Faris, Sophia, Mohamed Ghazouani, Hicham Medromi, and Adil Sayout. 2014. Information security risk assessment—A practical approach with a mathematical formulation of risk. *International Journal of Computer Application* 103: 36–42.

Frank, Michele L., Jonathan H. Grenier, and Jonathan S. Pyzoha. 2019. How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. *Journal of Information Systems* 33: 183–200. [CrossRef]

Ganin, Alexander A., Phuoc Quach, Mahesh Panwar, Zachary A. Collier, Jeffrey M. Keisler, Dayton Marchese, and Igor Linkov. 2020. Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis* 40: 183–99. [CrossRef]

Goel, Rajni, Anupam Kumar, and James Haddow. 2020. PRISM: A strategic decision framework for cybersecurity risk assessment. *Information & Computer Security* 28: 591–625.

Gordon, Lawrence A., and Martin P. Loeb. 2002. The Economics of Information Security Investment. *ACM Transaction on Information and System Security (TISSEC)* 5: 438–57. [CrossRef]

Gordon, Lawrence A., Martin P. Loeb, and Lei Zhou. 2020. Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity* 6: tyaa005. [CrossRef]

Hom, Jane, Boonsri Anong, Kim Beom Rii, Lee Kyung Choi, and Kenita Zelina. 2020. The Octave AllegroMethod in Risk Management Assessmnet of Educational Institute. *Aptisi Transactions on Technopreneurishp (ATT)* 2: 167–79. [CrossRef]

Kandasamy, Kamalanathan, Sethuraman Srinivas, Krishnashree Achuthan, and Venkat P. Rangan. 2020. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security* 2020: 1–18. [CrossRef]

Kaur, Gurdip, and Arash Habibi Lashkari. 2021. Information Technology Risk Management. In *Advances in Cybersecurity Management*. Cham: Springer International Publishing, pp. 269–87.

Kure, Halima Ibrahim, and Shareeful Islam. 2019. Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Physical Systems Theory & Applications* 4: 332–40.

Lee, In. 2020. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet* 12: 157. [CrossRef]

Lee, In. 2021. Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons* 64: 659–71. [CrossRef]

Mazzoccoli, Alessandro, and Maurizio Naldi. 2020. Robustness of optimal investment decisions in mixed insurance/investment cyber risk management. *Risk Analysis* 40: 550–64. [CrossRef]

McCarthy, Charlie, and Kevin Harnett. 2014. *National Institute of Standards and Technology (nist) Cybersecurity Risk Management Framework Applied to Modern Vehicles*. No. DOT HS 812 073. Washington, DC: National Highway Traffic Safety Administration.

Melaku, Henock Mulugeta. 2023. Investigating Potential Vulnerability of Critical Infrastructure and Way Forward—Recommendations to Enhance Security and Resilience. *Biomedical Science and Clinical Research* 2: 61–67.

Ni, Shentong, Yang Tang, Guorong Wang, Liu Yang, Bo Lei, and Zhidong Zhang. 2022. Risk identification and quantitative assessment method of offshore platform equipment. *Energy Reports* 8: 7219–29. [CrossRef]

Pandey, Shipra, Rajesh Kumar Singh, Angappa Gunasekaran, and Anjali Kaushik. 2020. Cyber security risks in globalized supply chains: Conceptual framework. *Journal of Global Operations and Strategic* 13: 103–28. [CrossRef]

Rampini, Gabriel Henrique Silva, Harmi Takia, and Fernando Tobal Berssaneti. 2019. Critical success factors of risk management with the advent of ISO 31000 2018-Descriptive and content analyzes. *Procedia Manufacturing* 39: 894–903. [CrossRef]

Rostamzadeh, Reza, Mehdi Keshavarz Ghorabaee, Kannan Govindan, Ahmad Esmaeili, and Hossein Bodaghi Khajeh Nobar. 2018. Evaluation of sustainable supply chain risk management using an integrated fuzzy TOPSIS-CRITIC approach. *Journal of Cleaner Production* 175: 651–69. [CrossRef]

Shad, Muhammad Kashif, Fong-Woon Lai, Chuah Lai Fatt, Jiří Jaromír Klemeš, and Awais Bokhari. 2019. Integrating sustainability reporting into enterprise risk management and its relationship with business performance: A conceptual framework. *Journal of Cleaner Production* 208: 415–25. [CrossRef]

Sheehan, Barry, Finbarr Murphy, Martin Mullins, and Cian Ryan. 2019. Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation research part A: Policy and Practice* 124: 523–36. [CrossRef]

Spross, Johan, Lars Olsson, Håkan Stille, Staffan Hintze, and Olle Båtelsson. 2022. Risk management procedure to understand and interpret the geotechnical context. *Georisk: Assessment and Management of Risk for Engineered Systems and Geohazards* 16: 235–50. [CrossRef]

Sulistyowati, Diah, Fitri Handayani, and Yohan Suryanto. 2020. Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. *JOIV International Journal on Informatics Visualization* 4: 225–30. [CrossRef]

Tranchard, Sandrine. 2018. Risk management: The new ISO 31000 keeps risk management simple. *Governance Directions* 70: 180–82.

Tupa, Jiri, Jan Simota, and Frantisek Steiner. 2017. Aspects of risk management implementation for Industry 4.0. *Procedia Manufacturing* 11: 1223–30. [CrossRef]

Uddin, Md Hamid, Md Hakim Ali, and Mohammad Kabir Hassan. 2020. Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Management* 22: 239–309. [CrossRef]

Vitunskaite, Morta, Ying He, Thomas Brandstetter, and Helge Janicke. 2019. Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security* 83: 313–31.

Wang, Dayu, Daojun Zhong, and Liang Li. 2022. A comprehensive study of the role of cloud computing on the information technology infrastructure library (ITIL) processes. *Library Hi Tech* 40: 1954–75. [CrossRef]

Woods, Daniel W., and Rainer Böhme. 2021. SoK: Quantifying cyber risk. Presented at 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 24–27 May, pp. 211–28.

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.