IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 787
 Journal Volume 10, Iss 08, 2021

A STUDY ON THE EVALUATING THE SECURITIES' RISK MANAGEMENT PRACTICES, INCLUDING IDENTIFICATION, MITIGATION, AND MONITORING ACROSS VARIOUS RISK CATEGORIES

[1]Bharath Kundala, [2]Ravi Chelimela,[3] Malika Apku, [4]G. Chakradhar

[1,2,3,4]Assistant Professor

Department of MBA

Kshatriya College of Engineering

Abstract:

The large amount of information handled by organizations has increased their dependance on information technologies, which has made information security management a complex task. This is mainly because they cover areas such as physical and environmental security, organization structure, human resources and the technologies used. Information security frameworks can minimize the complexity through the different documents that contain guidelines, standards, and requirements to establish the procedures, policies, and processes for every organization. However, the selection of an appropriate framework is by itself a critical and important task, as the framework must adapt to the characteristics of an organization. In this paper, a general vision of the newest versions of the NIST CSF, ISO/IEC 27001:2022, and MAGERIT frameworks is provided by comparing their characteristics in terms of their approaches to the identification, assessment, and treatment of risks. Furthermore, their key characteristics are analyzed and discussed, which should facilitate the consideration of any of these frameworks for the risk management of complex manufacturing organizations. **Keywords:** RMF; risk management; cybersecurity; ISO/IEC 27001; NIST CSF; MAGERIT

1. Introduction

A fundamental aspect of Industry 4.0 (I4.0) is the enhanced interconnectivity of networks that utilize the Internet of Things (IoT) and the Internet of Services (IoS) via cyberphysical systems. In this context, the IoT refers to physical devices that are equipped with microchips, software, sensors, and controllers that enable them to gather data. By contrast, the IoS is concerned with the transmission of data via the internet [1].

After I4.0, the European Commission introduced Industry 5.0 (I5.0) as a response to societal challenges, aiming to prioritize human values and contribute to society's needs. I5.0 is a transition to a sustainable, resilient, and human-centric industry, respecting production limits and workers' well-being [2]. The shift from Industry 4.0 to Industry 5.0 requires updating enabling technologies and creating new applications. This transition is essential for creating new value from critical rethinking of human resource [3]. The I5.0 vision takes efficiency and productivity to the next level by putting the worker at the center of the production process and prioritizing sustainability.

The latest improvements in information and communication technologies have

increased the use of I4.0 and I5.0. These developments have led to new cybersecurity risks that organizations need to tackle. Over the past few years, the number of cyberattacks has surged, and organizations are implementing measures to mitigate the damages caused by these attacks [4,5]. This, in turn, has made data management and security one of the key facilitators of its realization [6,7]. Indeed, this has propagated the need to research new concepts and methods that allow us to increase and optimize the level of security information [8]. Therefore, authors such as Culot et al. [9] mention the need for information security systems that can handle a holistic approach to face the complex challenges of today. Agrawal [10] discusses some of the reasons why organizations should classify information, among them being the protection of confidential information, contractual compliance, compliance with regulations and the acquisition of competitive advantages. On the other hand, Azmi [11] mentions that international organizations, countries, companies, and academic institutions have actively worked to develop cybersecurity frameworks to achieve cyber resilience. Dawson [12] defines cybersecurity frameworks as those that provide policies and procedures for the application and continuous management of information security controls, providing frameworks that bring together elements such as education, policies and technologies, adapting to preestablished requirements and also controlling emerging requirements.

Lopes et al. [13] discuss how some of the advantages of implementing information security systems, such as the ISO/IEC 27001, are the identification and elimination of threats and vulnerabilities, a greater confidence in the interested parties, better awareness in terms of security, and an increase in the ability to anticipate, manage and survive a catastrophe. This guarantees business continuity, reducing the costs associated with non-security and complying with current legislations. On the other hand, Cockcroft and Ferruzola et al. [14,15] mention that the implementation of a cybersecurity framework can be seen as an advantage when it comes to integrating business and cybersecurity risk management, these being validated by the top management, thereby maintaining an updated understanding of the cybersecurity risk.

The selection of cybersecurity frameworks for complex manufacturing organizations should be made after carefully considering several factors. This is primarily because complex manufacturing organizations require a comprehensive approach to risk management that takes into account both structured and unstructured data. Additionally, the selected frameworks must have demonstrated their effectiveness in similar contexts and have gained industry recognition as best practices. This paper provides a systematic review of cybersecurity frameworks, such as ISO/IEC 27001:2022, NIST CSF, and MAGERIT, with a focus on their risk management methodologies. By comparing and contrasting the key characteristics and proposed controls of these frameworks, this study aims to answer the following research question: “What are the key characteristics and differences between the risk management methodologies of the ISO/IEC 27001:2022, NIST CSF, and MAGERIT frameworks, and how can they be applied effectively in complex organizations in I4.0 and I5.0”? This review aims to provide insights into how the ISO/IEC 27001:2022, NIST CSF, and MAGERIT

frameworks can be applied effectively in complex organizations in I4.0 and 5.0. By analyzing their strengths and weaknesses, this paper offers a comprehensive understanding of the advantages and disadvantages of each framework in terms of the risk management strategies. The results of this study will be useful for organizations seeking to implement effective risk management strategies that consider the unique challenges posed by the enhanced interconnectivity of networks utilizing IoT and IoS via cyber-physical systems.

The rest of the manuscript is organized as follows. In Section 2, a literature review is presented where an analysis of published works is provided to denote the increase in publications related to cybersecurity frameworks. In Section 3, a comparison of the security management frameworks is presented based on the ISO/IEC 27001:2022, NIST CSF and MAGERIT frameworks. In Section 4, a comparison is provided of the risk management strategies, which covers the identification, assessment, treatment, and control of risks in these three frameworks. In Section 5, a discussion about the characteristics of the three considered frameworks is presented. Finally, in Section 6, the conclusions are given.

2. Literature Review

The emergence of Industry 4.0 and its associated technologies has resulted in new risks for organizations [16]. Given this, organizations are dealing with a rise in cyber threats and the associated costs related to information security. For instance, the number of attacks on IoT devices has grown considerably [17]. However, Griffy et al. [18] argue that these problems are never tackled in isolation in the business world, and hence, it is crucial to take a wider perspective given the agility that more and more companies use.

According to Falivene and Tucker [19], it is crucial to identify cybersecurity frameworks that go beyond a mere checklist of best practices and avoid those that make even expert-level tasks more complicated. Azmi [11], therefore, aims to integrate different viewpoints on cybersecurity frameworks by using descriptive and pattern coding to create a brief version that covers the action encouraged, the framework's driver, environment, and intended audience. Additionally, cybersecurity could be addressed by focusing on the five pillars, which include human, organizational, infrastructure, technology, and legal and regulatory aspects.

Tatiara et al. [20] study the factors that impede the adoption of information management systems and find that success depends on the involvement of all parties in the implementation process. They recommend involving top management, regularly communicating employee policies, conducting periodic reviews of the implementation of Information Security Management Systems (ISMS), keeping employees informed of any improvements, clearly communicating roles, responsibilities, and authorities related to ISMS to employees on a regular basis, developing work programs for the implementation of information security systems and distributing them to staff, and frequently announcing information security policies and objectives to employees.

Information security management frameworks enable the inclusion or combination of various processes within their context to meet the requirements of the organizational context. They provide

ISSN PRINT 2319 1775 Online 2320 787
 Journal Volume 10, Iss 08, 2021

specific taxonomies for categorizing risks, enabling organizations to modify, retain, avoid or share risks as per their needs [21].

Research Methodology

Cybersecurity frameworks are inherently complex and can be analyzed from various research perspectives. In order to mitigate this complexity, we have opted for a systematic approach in our literature review, guided by the methodological recommendations of Tranfield et al., Xiao et al., and Lame et al. [22–24] as follows: 1. The research was carried out in two parts. Firstly, the data were obtained from "Google Scholar". 2. Initially, we used the keyword "Cybersecurity Frameworks" to identify the most common cybersecurity frameworks. 3. From the first publication of 2018 to March 2023. 4. Document type "Article and Review". The search yielded 101 articles, among which the most mentioned frameworks were

NIST CSF and ISO/IEC 27001

In the second part of the research, the keywords "NIST CSF" and "ISO/IEC 27001" were searched in the "Scopus", "IEEE", and "Google Scholar" databases. Additionally, the keyword "MAGERIT" was included to identify the scope and limitations of this methodology, which is being used in Spain and Latin America. The same date range and criteria were used for the reviewed articles, resulting in 13,359 articles. Articles without peer review were excluded and the articles were screened for duplicates, reducing the number to 498 articles. Of these, 30 were not written in English or Spanish, leaving 468 articles. Another screening of the titles, keywords, and abstracts was performed, resulting in the selection of 94 articles. Finally, irrelevant articles to the main topic and those that did not have the recommended frameworks were eliminated, resulting in 50 articles. The entire process is illustrated in Figure 1 using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) diagram.

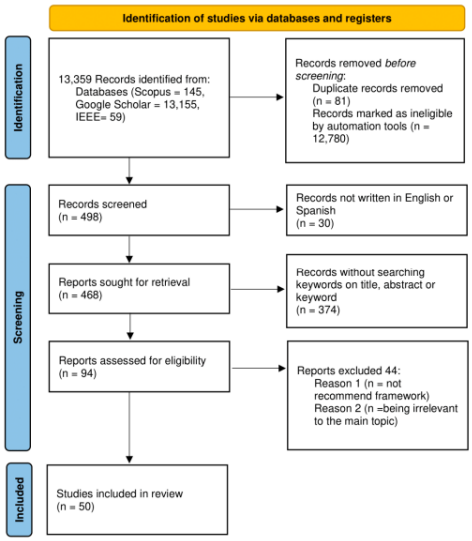

Figure 1. PRISMA flow diagram

Figure 2 shows a steady increase in the number of articles published each year from 2018 to 2023. In 2018, there were 60 articles published, while in 2019, the number of articles increased to 72. In 2020, there was a significant increase in the number of articles, with 95 articles being published. This trend continued in 2021, with a further increase to 102 articles, followed by 112 in 2022.

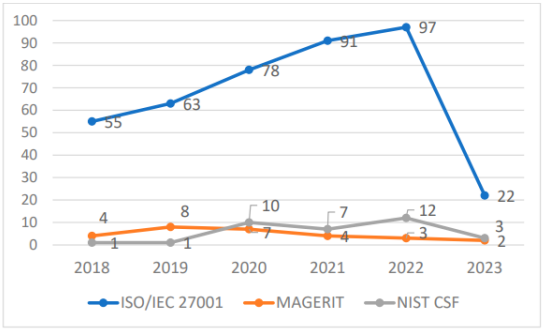

Figure 2. Publication rate of common cybersecurity frameworks in "Google Scholar", "IEEE", and "Scopus".

As of March 2023, there were already 27 articles published, indicating that the trend is expected to continue. It is important to note that the graph only shows the number of articles published in the range of 2018–2023 and does not include any articles published before or after this period. Overall, the graph shows a significant increase in the number of publications in the field of cybersecurity frameworks such as NIST CSF, ISO/IEC 27001 and MAGERIT, indicating the growing interest in and importance of this field in recent years. Table 1 provides an exhaustive list of the most significant documents in the literature, carefully selected based on the criteria outlined earlier. The documents have been rigorously analyzed and classified into four distinct categories to enable ease of access and comprehension for the reader.

Table 1. Relevant documents in the literature.

	ISO/IEC 27001	NIST CSF	MAGERIT
Literature review	[9,25,26]	[27,28]	[29–31]
Methodology comparison		[32–36]	
Case studies	[37,38]	[39–42]	[15,43,44]
Implementation Guides	[13,20,45–48]	[49–51]	-

These categories are as follows:

1. Literature review: This category comprises comprehensive literature reviews, encompassing both qualitative and quantitative studies, which provide a broad understanding of the current state of knowledge on a particular topic.

2. Comparison of methodologies: This category includes studies that compare and contrast different research methodologies, highlighting the strengths and weaknesses of each approach.

3. Case studies: This category comprises in-depth analyses of specific cases, providing a detailed understanding of the subject matter in question and offering insights that may be applicable to similar situations.

4. Implementation guides: This category includes practical guides that provide stepby-step instructions on how to implement specific methodologies or approaches in practice, highlighting potential challenges and offering advice on how to overcome them.

In summary, Table 1 presented herein aims to serve as a valuable resource for researchers and practitioners alike, providing a comprehensive overview of the most relevant documents in the literature and enabling the identification of useful information and insights for their respective areas of interest.

The importance of information security management frameworks is increasing due to the rising number of threats to sensitive data. Organizations are advised to combine the best practices of various frameworks to create a comprehensive security framework suitable for their unique needs and resources. Lopes (2019) and Diamantopoulou (2020) [13,45] highlight that organizations that already have an ISMS in place not require a duplication of effort to meet the General Data Protection Regulation (GDPR) requirements. Mylrea (2018) [50] suggests that organizations with mature, proactive insider threat programs are better positioned to identify, detect, and mitigate these threats.

The commonly used frameworks include NIST CSF, ISO/IEC 27001:2022 [52], and MAGERIT [53], the latter of which is gaining acceptance in Latin America due to its easy language and risk management process based on ISO/IEC 31000 [40,47]. The following section will compare these frameworks to help organizations select the most appropriate one for their needs.

ISSN PRINT 2319 1775 Online 2320 787
 Journal Volume 10, Iss 08, 2021

3. A Comparison of Information Security Management Frameworks

As risk management continues to gain importance within organizations, it is recommended to combine the best practices of various frameworks rather than choosing one over another [35]. This approach can result in a more comprehensive security framework that is tailored to the organization and its available resources. Information security methodologies are critical for safeguarding an organization's sensitive data and information. These methodologies include a set of processes and techniques to identify, assess, and mitigate information security risks. Among the most commonly used are the NIST CSF, ISO/IEC 27001:2022, and MAGERIT.

The NIST CSF uses a universal and comprehensible language that adjusts to diverse technologies, sectors, and purposes. It is based on risk and global standards, and it was created from various perspectives of the private, academic, and public sectors. The framework includes five functions: Identify, Protect, Detect, Respond, and Recover. Figure 3 illustrates the functions that depict the desired results using clear and easily comprehensible language, thus rendering it relevant to all forms of risk management.

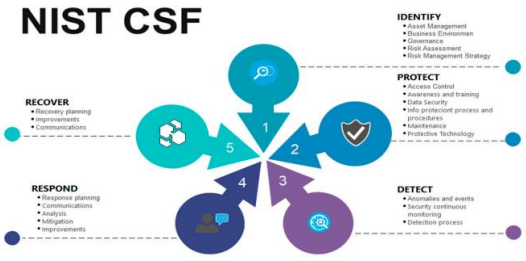

Figure 3. Functions of NIST CSF

Longras et al. [48] conclude that the implementation and certification of ISO/IEC 27001 can be challenging due to various factors, such as the financial cost, lack of implementation examples, difficulty in defining scope, setbacks in the interpretation of the standard and documentation, resistance to change, and allocating roles or tasks to different employees. Implementing an ISMS requires significant effort and changes in the organization's activity, and organizations must perform a set of policies to comply with legal requirements. However, the benefits of certification include increased compliance with legal requirements, improved customer and competitive advantages, greater effectiveness, and efficient investments to reduce security incidents [48].

The MAGERIT methodology is freely accessible and can be used without permission. It is especially useful for organizations that fall under the National Security Scheme (ENS), as it helps them comply with risk management and analysis principles. On the other hand, MAGERIT is beneficial for entities that rely heavily on information technologies to achieve their organizational goals and objectives. The methodology is composed of three books that cover the method, catalog of elements, and technical guidelines.

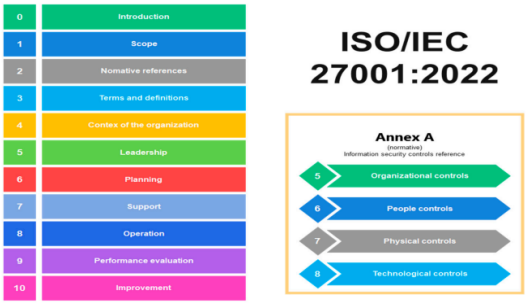

Figure 4. Sections of ISO/IEC 27001:2022

MAGERIT aligns with the ISO 31000 terminology and focuses on implementing the "Risk Management Process". It also provides a working framework for

ISSN PRINT 2319 1775 Online 2320 787
 Journal Volume 10, Iss 08, 2021

governing bodies to make informed decisions by considering the risks associated with the use of information technologies. The objective of Table 2 is to compare the NIST CSF 1.1, ISO/IEC 27001:2022, and MAGERIT v.3 methodologies. The comparison categories were determined based on recommendations from articles such as [54,55] as well as the main components of each of the frameworks in order to outline their key characteristics, similarities and differences. In the first instance, it can be noted that the ISO/IEC 27001:2022 framework has the most recent update in August 2022, while NIST CSF 1.0 was initially produced in 2014, updated in 2018 to NIST CSF 1.1, and is currently being updated in an open manner with input from various sectors. The latest update, NIST CSF 2.0, is still in a concept paper and is expected to be implemented by winter 2024, depending on the community's needs, while MAGERIT v.3 has not been updated since October 2012. The structures of the three frameworks are configured differently. ISO/IEC 27001:2022 consists of 11 sections, of which 0 to 3 are optional, and includes Annex A, which outlines potential controls that may be used depending on the organization. MAGERIT's structure is more similar to ISO/IEC 27001:2022, as it shares the ISO 31000 risk management structure and approaches security risk management holistically. This approach promotes adaptability, goal orientation, multi-stakeholder involvement, and continuous improvement through a systemic approach. By contrast, NIST is based on five interconnected functions that help organizations comprehend security risks, safeguard their systems and data, detect threats, respond to incidents effectively, and recover from them. The NIST CSF, ISO/IEC 27001:2022, and MAGERIT cybersecurity frameworks are built upon the foundation of risk management. This pivotal process entails identifying, evaluating, and minimizing risks to uphold an acceptable level. In the domain of risk management, ISO/IEC 31000 functions as a fundamental reference. In the next section, we will expound upon some significant concepts associated with risk management, along with the methodologies employed by the aforementioned cybersecurity frameworks.

Table 2. Comparison of information security management frameworks

	ISO/IEC 27001	NIST CSF	MAGERIT
Updated	August 2022	April 2018	October 2012
Description	International standard describing best practices for an information security management system.	Security framework for the protection of operations and assets.	Security framework that seeks to raise awareness of the existence of risks and the need to manage them in organizations.
Structure	11 sections, 0–3 non-mandatory and 4–10 mandatory, Annex A.	5 functions, 22 categories and 98 subcategories, 4 levels of implementation.	9 categories, 6 appendices, catalog of elements and guide to techniques
Certifiable	Yes	No	No
Mandatory documents	Clauses 4 to 10	Not specified	Not specified
Based	Risk management	Risk management	Risk management
Mechanisms	Non-voluntary and independent audit	Optional, self-certification	Optional, self-certification.
Scope	Provides the requirements for establishing, implementing, maintaining, and continuously improving an information security management system, as well as the requirements for assessing and addressing information security risks tailored to the needs of organizations.	Optional guidelines, best practices, and standards for improving cybersecurity programs.	Implements the risk management process within a framework for the governing bodies to make decisions, taking into account the risks derived from the use of information technologies.
Technology independence	Yes	Yes	Yes
Availability	Distributed commercially	Free download from the official website	Free download from the official website

4. Risk Management Methodologies

Risk management is an essential process that involves the ongoing identification, assessment, and mitigation of risks to maintain an acceptable level. It is a broad term that encompasses risk assessment as one of its components. Risk management involves the development, implementation, and monitoring of strategies to mitigate or transfer risks to an acceptable level. ISO/IEC 31000 serves as a fundamental reference when discussing risk management. This document defines risk management as a coordinated effort to monitor and regulate the relationship with risks. In this sense, risk is defined as the result of uncertainty regarding objectives, which can have positive or negative consequences and can manifest as opportunities or threats [56]. Objectives

may vary in their type and category, and risk management can be conducted at various levels. Risk management ought to be an integrated process within an organization's overall management rather than a separate or isolated activity. This integration ensures that risk management becomes a standard practice and is conducted consistently and effectively [57].

Risk management models differ in their form and structure, although most models adhere to a systematic approach that includes policies, procedures, and practices for communication and consultation activities. This approach also entails a risk assessment process consisting of preparation, evaluation of risk factors, assessment or determination of risk, and control or treatment of the risk [58]. Risk management involves comprehending the characteristics of a risk, including identifying when it is acceptable to take that risk. This procedure involves evaluating multiple elements, such as chance, potential risk sources, results, likelihoods, circumstances, scenarios, and the efficiency of preventive measures [57].

When addressing risk, a process of selecting and executing solutions is employed, involving multiple cycles that must include formulating and selecting options, planning and implementing actions, evaluating their effectiveness, determining the acceptability of the risk, and, if not accepted, undertaking additional treatments [57]. In Sections 4.1–4.3, we present some of the key features of the risk management methodologies.

ISO/IEC 27001:2002 (ISO27005), NIST CSF (NIST SP 800-30, NIST SP 800-37, NIST SP 800-39), and MAGERIT (MAGERIT). In Section 4.4 and its subsections, we compare the risk management processes of these methodologies.

4.1. ISO/IEC 27005:2022 ISO/IEC 27001 recommends that organizations establish a risk management process that is appropriate for their context, implement controls to mitigate identified risk, and continually monitor and review the effectiveness of these controls. ISO/IEC 27005:2022 provides a guide to risk management and offers a systematic and structured approach to managing risk and establishing and maintaining an effective risk management program. This document is titled "Guidance on Information Security Risk Management for Information Security, Cybersecurity, and Privacy Protection." Its purpose is to offer advice that assists organizations in the following:

• Fulfilling the actions required by ISO/IEC 27001:2022 to address information security risks.

• Carrying out ISMS activities, particularly evaluating and assessing information security.

This document, which is now in its fourth edition under the name ISO/IEC 27005:2022, applies to all organizations regardless of their industry, size, or type. The primary modifications made to this edition compared to the 2018 third edition are that it is structured to align with ISO/IEC 27001:2022, employs terminology from ISO 31000:2018, introduces the concept of risk scenarios, presents a comparison of the event-based and asset-based approaches to risk identification, and consolidates the annexes into a single one. It offers advice on fulfilling the ISO/IEC 27001 requirements and provides actions to address information security risks, detailed guidance on risk management, and

instructions on applying the ISO 31000 risk management guidelines in the context of information security. It can also be used by individuals involved in information security risk management or by organizations seeking to improve their information security risk management process. Its main aim is to assist organizations in safeguarding their valuable information assets, such as confidential and sensitive data.

Figure 5 illustrates the ISO/IEC 27005:2022 process that is carried out by following these steps:

1. Establishing the context, which includes identifying and defining the scope, determining the criteria for risk acceptance, and identifying any legal, regulatory, or contractual requirements.

2. Conducting a risk assessment, which includes the following:

a. Identifying risks. Identifying the risks that could affect the CIA of the information assets.

b. Analyzing risks. By assessing the likelihood and impact of the risks based on the identified threats, vulnerabilities, and the existing controls.

c. Evaluating risks. Evaluating the risks by comparing the assessed risks with the established risk criteria, which include the risk appetite and the risk tolerance of the organization.

3. Treating iteratively the identified risks. Implementing controls or taking other actions to reduce the likelihood or impact of the risk.

4. Implementing risk management processes. Establishing communication channels, and monitoring and reviewing the risk management process.

5. Utilizing management system processes. Integrating the risk management process with other management systems, such as quality or environmental management.

6. Documented information. Document all relevant information, such as risk assessments, treatment plans, and management system processes.

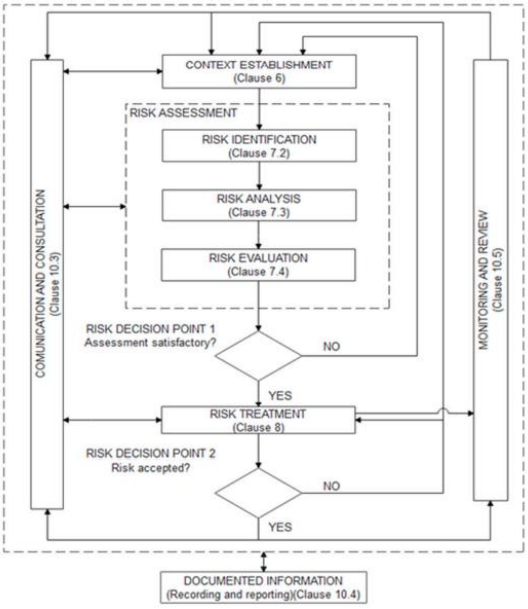

Figure 5. Risk management process for ISO/IEC 27005:2022. Adapted with permission from ref. [59]. Copyright remains with ISO.

4.2. NIST SP 800-30, NIST SP 800-37 and NIST SP 800-39

NIST CSF incorporates risk assessment as part of its cybersecurity implementation process, although it does not specify a particular risk management methodology. In addition to the CSF, NIST has released several publications, such as NIST SP 800-30, NIST SP 800-37, and NIST SP 800-39, that address several aspects of risk management. NIST SP 800-30 provides guidance for conducting information security risk assessments, including identifying assets, threats, and vulnerabilities, and determining the

ISSN PRINT 2319 1775 Online 2320 787
 Journal Volume 10, Iss 08, 2021

likelihood and impact of risks. NIST SP 800-30 focuses on identifying and assessing risks to information systems and how those risks may impact the organization. The last version of NIST SP 800-30, Rev. 1, was published in July 2012 [60]. NIST SP 800-37 offers a detailed description of the risk management framework (RMF) and provides guidance on how to apply it to information systems and organizations. The RMF is a rigorous and adaptable process for managing security and privacy risks, encompassing the categorization of information security, the selection of appropriate controls, their implementation and evaluation, the authorization of system and common controls, and continuous monitoring. The focus of NIST SP 800-37 is on the implementation of the RMF and how risks can be effectively managed throughout the entire information system life cycle. The latest version of NIST SP 800-37, Rev. 2, was published in December 2018 [51].

NIST SP 800-39 provides guidelines for enterprise-wide IT risk management. This publication focuses on organization-wide IT risk management, including the assessment and management of IT risks that may impact the organization as a whole. NIST SP 800-39 also includes the management of IT risks related to external vendors and third parties, as well as the management of information security incidents. The last version of NIST 800-39, Rev. 2, was published in November 2019. Figure 6 provides a short description of the steps involved in implementing NIST SP 800-39 [61].

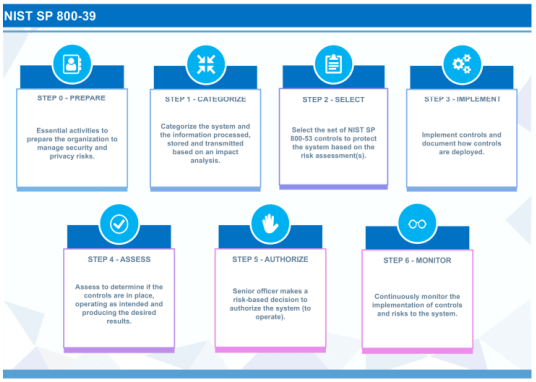

Figure 6. Steps for implementing NIST 800-39.

3. MAGERIT

The CSAE (Consejo Superior de Administración Electrónica) created and advocates for MAGERIT, recognizing the growing significance of information systems for both public administration and society as a whole in achieving their goals. Robust security measures must be implemented to manage these systems and maintain the confidence of service users. The objective of MAGERIT is to raise awareness among organizations about the need to manage risks systematically, with the aim of keeping them under control and preparing for evaluation, audit, certification, or accreditation processes. The methodology aims to ensure uniformity in the reports that include the findings and conclusions of the risk analysis and management activities. Ultimately, MAGERIT aims to implement security measures that support the confidence of users of services. The methodology is composed of three main stages, which are as follows

After analyzing the ISO/IEC 27001, NIST CSF, and MAGERIT standards, it is evident that effective risk management is a critical component of a robust information security program. In summary, risk management is the process of identifying, assessing, and prioritizing risks and

ISSN PRINT 2319 1775 Online 2320 787
 Journal Volume 10, Iss 08, 2021

implementing strategies to mitigate or eliminate those risks. It involves identifying potential threats, vulnerabilities, and assets at risk, assessing the likelihood and potential impact of each risk, and developing and implementing controls to manage or eliminate them.

4.4. Risk Management Process Comparison

By using a risk management approach, organizations can prioritize their security efforts and focus on the most critical areas. The risk management process should be an ongoing, iterative process that adapts to changing threats and business needs. Overall, it is a vital part of any organization's security program. The goal of risk management is to develop and implement strategies that reduce the likelihood and impact of identified risks. Sections 4.4.1–4.4.3 elaborate on how NIST CSF, ISO/IEC 27001:2022 and MAGERIT undertake these processes by highlighting the similarities and differences among.

4.4.1. Identifying Potential Risks

To safeguard information security in any organization, it is crucial to identify potential risks. The ISO/IEC 27001:2022, NIST 800-39, and MAGERIT methodologies employ a series of procedures to achieve this goal. Table 3 summarizes the key steps involved in risk identification. These steps involve comprehending the context, recognizing critical processes and assets, identifying possible threats and vulnerabilities, evaluating the probability and impact of risks, prioritizing them, and devising response plans. ISO/IEC 27001:2022, NIST CSF, and MAGERIT provide guidance on risk identification and management, with ISO/IEC 27001:2022 focusing on identifying risks to the CIA of information, NIST CSF focusing on identifying risks to critical infrastructure and information systems, and MAGERIT focusing on identifying, assessing, and prioritizing risks to information systems, including identifying potential attackers or actors responsible for an attack. The frameworks suggest various techniques and methodologies, such as threat catalogs or analysis techniques, including SWOT (Strengths, Weaknesses, Opportunities, and Threats) or FMEA (Failure Mode and Effect Analysis), the NIST SP 800-30, NIST SP 800-37 or NIST SP 800-39 documents, and the MAGERIT methodology, to help identify relevant risks and vulnerabilities.

Table 3. Process of risk identification for each methodology.

Risk Identification	ISO/IEC 27001:2022	NIST	MAGERIT
Understanding the Context	Understand the scope and objectives of the information system to identify critical assets.		
Process identification	The organization is responsible for the ongoing management of an ISMS, including the necessary processes and their interrelationships, to comply with the requirements established in this document.		Identify critical processes to be protected and relevant assets.
Identify Threats	Use standard threat catalogs or analysis techniques such as FMEA or SWOT to identify potential threats.	Use the NIST framework to identify relevant threats, such as NIST SP 800-30, NIST SP 800-37 or NIST SP 800-39.	Use the MAGERIT methodology to identify relevant threats, including the identification of actors that could be responsible for an attack.
Vulnerability Identification	Identify weaknesses or weak points in the system that can be exploited by threats.		
Impact Assessment	Determine the potential impact on assets and the business in the event of a security incident.		
Probability Evaluation	Determine the probability of a threat exploiting a vulnerability and causing an impact.		
Risk Prioritization	Prioritize risks based on the combination of impact and probability.		
Response Planning	Develop a plan to mitigate or address identified and accepted risks.		

4.4.2. Risk Assessment

Risk assessment is the process of identifying, analyzing, and evaluating risks to determine the likelihood and potential impact of those risks. The main goal of risk assessment is to identify potential risks and provide information that can be used to make in-formed decisions about how to manage those risks [62]

Risk assessment processes commonly utilize qualitative assessment methods, which rely on subjective understanding and evaluation of risks. However, the results obtained from these methods may be somewhat subjective. By contrast, quantitative methods employ specific risk

indicators, resulting in more objective and reasonable outcomes based on numerical data and statistics. Hybrid methods exist that combine aspects of both the qualitative and quantitative approaches, effectively addressing the complexity of risk assessment. These methods have also been expanded to handle uncertainty factors and evaluate safety risks in financial terms [58,63].

In this phase, the likely impact of every potential threat on each of the recognized assets is assessed, taking into account the CIA and non-repudiation of the information. While this step is not typically part of the risk assessment process, it can be inferred from appropriate security measures implemented to safeguard the CIA of the information. The latter is a crucial aspect, although it is not specifically evaluated directly in the risk assessment. Risk assessment is founded on threat assessment, which involves identifying potential vulnerabilities and the ways in which they could be exploited. A threat vector, on the other hand, refers to the path taken by an attacker to target the system. Threat sources are categorized into four types—adversarial, accidental, structural, and environmental—which can be either internal or external.

• Adversarial threats originate from individuals, groups, organizations, or nations. • Accidental threats refer to unintentional actions.

• Structural threats are caused by equipment or software failures.

• Environmental threats arise from external disasters, which can be either natural or human-made, such as fires and floods.

• Assessing the likelihood of an attack originating from a human threat source can be challenging and may involve evaluating factors such as skill level, motive, opportunity, and size.

• Vulnerability assessment, on the other hand, takes into account several factors, such as exploitability, ease of detection, intrusion detection, and awareness. A combination of historical and estimated data should be used to provide the most accurate probability of an event occurring.

• The magnitude of impact should be determined, which can be classified on a scale ranging from very low to very high or negligible to catastrophic impact.

4.4.3. Treatment and Control

The ISO/IEC 27001:2022 and MAGERIT guidelines emphasize that the selection of a control must be based on the results and conclusions derived from the risk analysis and assessment process. Figure 7 shows the control measures, which are categorized by family in each of the standards. ISO/IEC 27001:2022 classifies them into four categories, while NIST 800-53 Rev. 5 has 20 categories, and MAGERIT has 16 categories, which are quite similar to those of NIST, with minor variations in the naming conventions of the categories. The figure shows a short description of these categories per family

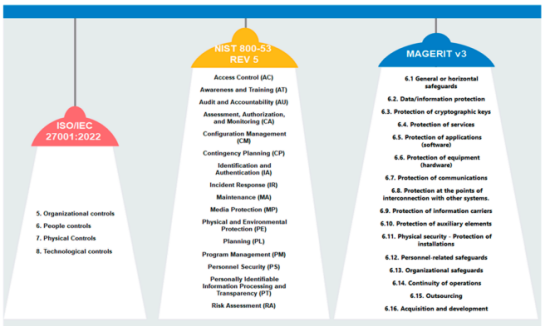

Figure 7. Controls categories by framework.

Discussion

ISSN PRINT 2319 1775 Online 2320 787
 Journal Volume 10, Iss 08, 2021

Risk management is an indispensable process for maintaining information security in any organization. There are several methodologies available for conducting risk management, each with its own unique approach and characteristics. This section aims to Figure 7. Controls categories by framework. 5. Discussion Risk management is an indispensable process for maintaining information security in any organization. There are several methodologies available for conducting risk management, each with its own unique approach and characteristics. This section aims to highlight the distinctions between three frameworks, ISO/IEC 27001:2022, NIST CSF and MAGERIT, and provide recommendations for selecting a specific approach based on particular circumstances. ISO/IEC 27001:2022 is centered on information security management and prioritizes the identification of information assets, evaluation of the associated risks, and implementation of relevant control measures. One of the advantages of ISO/IEC 27001:2022 is its structured and process-oriented approach, which facilitates effective and efficient information security management. However, the implementation of ISO/IEC 27001:2022 can be expensive and demands significant investments in terms of time and resources. When it comes to the IoT and IoS, ISO/IEC 27001 can be used to ensure the CIA of data exchanged through these systems. The standard can also be used to manage risks associated with the use of IoT and IoS devices in an organization's network.

The NIST CSF functions are presented in a user-friendly language that can be applied to various types of risk management. The framework is self-assessing and offers flexibility in the selection of a risk management methodology. Organizations can choose from among NIST's publications, such as NIST SP 800-30 for information security risk assessment, NIST SP 800-37 for the implementation of the information security risk management framework, and NIST SP 800-39 for enterprise-wide IT risk management. Alternatively, they can select any other methodology that meets their specific requirements. NIST CSF can be applied to the IoT and IoS to help organizations identify and manage the cybersecurity risks associated with these systems. For example, the Identify function can help organizations understand the types of IoT and IoS devices used in their networks, while the Protect function can help organizations secure these devices and the data they transmit.

MAGERIT, developed by the Spanish government, concentrates on managing information security risks in the public sector through a life cycle approach that covers identifying assets, threats, vulnerabilities, and risks, selecting security measures, implementing controls, and continually monitoring them. Its strength lies in its all-encompassing approach, which enables a thorough and methodical assessment of information security risks. Nonetheless, the MAGERIT approach may be too intricate for smaller and less complex organizations. MAGERIT can be used to manage risks associated with the IoT and IoS by identifying the assets, threats, vulnerabilities, and impacts of these systems. The framework can also be used to select appropriate controls to manage the risks associated with IoT and IoS devices.

The NIST CSF, ISO/IEC 27001, and MAGERIT frameworks can be applied to the IoT in a similar manner as they are

applied to other information systems. However, there are some specific considerations that need to be taken into account when applying these frameworks to the IoT. Some of these considerations are as follows: • Scalability: IoT systems can have a large number of devices, which can make it difficult to scale the application of these frameworks. • Diversity of devices: IoT devices come in different shapes, sizes, and functionalities. This can make it challenging to identify and classify all the risks associated with these devices. • Real-time nature: Many IoT systems operate in real time, which can make it difficult to implement some of the risk management processes outlined in these frameworks. • Data privacy: IoT devices generate a lot of data, and these data can be sensitive. Therefore, privacy and security considerations should be given a higher priority in IoT systems.

Despite these challenges, the frameworks can be applied to the IoT by adapting their application to the specific requirements of these systems. For example, risk assessments should be conducted regularly to identify new risks and to determine the effectiveness of existing controls. Additionally, security controls should be implemented in a layered approach to ensure that all the components of the IoT system are adequately protected. Finally, organizations should ensure that they have a clear understanding of the data that are being collected and stored by IoT devices and implement appropriate measures to protect these data.

In addition, the role of structured and unstructured data in complex organizations cannot be overstated, particularly when it comes to cybersecurity. With the exponential growth of data in recent years, it has become increasingly challenging for organizations to manage and secure their information effectively. In particular, unstructured data (data that lack a predefined data model or structure) pose a significant challenge [64]. Unstructured data can take many forms, including text documents, images, audio and video files, social media posts, and email messages. Such data are often generated and stored in disparate systems and locations, making the data difficult to track and secure. Furthermore, unstructured data are susceptible to cyber threats such as malware, phishing attacks, and data breaches. To address these challenges, these frameworks provide a structured approach to managing cybersecurity risks, including those associated with unstructured data. For example, ISO/IEC 27001 requires organizations to identify the types of information they process, including unstructured data, and implement appropriate controls to protect that information. MAGERIT might be used in a public organization to identify and assess the risks associated with both types of data. NIST CSF might be used to provide specific guidance on how to implement security controls for both structured and unstructured data in complex organizations.

To ensure information security and business continuity, organizations should evaluate their needs and choose a risk assessment methodology that aligns with their objectives and available resources. Smaller and less complex organizations may find ISO/IEC 27001 beneficial due to its structured and process-based approach. Conversely, larger and more complex organizations may prefer NIST CSF or MAGERIT, which offer a detailed and holistic approach. Ultimately, selecting a methodology and conducting a risk assessment are essential for all

organizations to protect their information assets and maintain business continuity

6. Conclusions

It should be emphasized that the implementation of cybersecurity frameworks for the IoT requires meticulous planning and execution, which involves identifying assets, evaluating risks, and establishing suitable security controls to safeguard the assets to ensure the sufficient protection of the devices and the data they handle and transmit.

The three information security standards, ISO/IEC 27001:2022, NIST CSF, and MAGERIT, have distinct approaches to information security management and are applicable in different geographic contexts and sectors. ISO/IEC 27001:2022 is a widely accepted international standard that focuses on information security management and provides guidelines for protecting and managing information and offers the option of certification to demonstrate compliance with the standard. NIST CSF, on the other hand, focuses more on implementing information security solutions and is more suitable for government organizations in the United States. MAGERIT, developed by the Spanish government, concentrates on risk assessment and management at the organizational level, and it can be applied to different types of organizations in Spain. In any case, the appropriate standard to use depends on the specific needs and objectives of the organization. Despite having some similarities, each standard has its own unique strengths and weaknesses, and choosing any of them can enhance an organization's information security. However, it is crucial to carefully consider which standard is most suitable for an organization's security needs and requirements. One recommendation for future work is studying the maturity of the cybersecurity frameworks of Mexican companies, which could be done through a data mining analysis of major organizations. This study would involve collecting and analyzing data related to cybersecurity practices, policies, and procedures from a sample of organizations in different sectors, such as finance, healthcare, and government. The analysis could focus on various aspects of cybersecurity, including risk management, threat detection and response, incident management, and employee training and awareness.

References

1. Burritt, R.; Christ, K. Industry 4.0 and environmental accounting: A new revolution? Asian J. Sustain. Soc. Responsib. 2016, 1, 23–38. [CrossRef]

2. Waheed, A.; Alharthi, M.; Khan, S.Z.; Usman, M. Role of Industry 5.0 in Leveraging the Business Performance: Investigating Impact of Shared-Economy on Firms' Performance with Intervening Role of i5.0 Technologies. SAGE Open 2022, 12, 21582440221094608. [CrossRef]

3. Golovianko, M.; Terziyan, V.; Branytskyi, V.; Malyk, D. Industry 4.0 vs. Industry 5.0: Co-Existence, Transition, or a Hybrid. Procedia Comput. Sci. 2023, 217, 102–113. [CrossRef]

4. Bakon, K.; Holczinger, T.; Sule, Z.; Jasko, S.; Abonyi, J. Scheduling under Uncertainty for Industry 4.0 and 5.0. IEEE Access 2022, 10, 74977–75017. [CrossRef]

5. Kumar, S.; Mallipeddi, R.R. Impact of cybersecurity on operations and supply chain management: Emerging trends and

future research directions. Prod. Oper. Manag. 2022, 31, 4488–4500. [CrossRef]

6. Raptis, T.P.; Passarella, A.; Conti, M. Data management in industry 4.0: State of the art and open challenges. IEEE Access 2019, 7, 97052–97093. [CrossRef]

7. Lowry, P.B.; Dinev, T.; Willison, R. Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. Eur. J. Inf. Syst. 2017, 26, 546–563. [CrossRef]

8. Dotsenko, S.; Illiashenko, O.; Kamenskyi, S.; Kharchenko, V. Integrated Security Management System for Enterprises in Industry 4.0. Inf. Secur. Int. J. 2019, 43, 294–304. [CrossRef]

9. 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]

10. Agrawal, V. A Framework for the Information Classification in ISO 27005 Standard. In Proceedings of the 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017, New York, NY, USA, 26–28 June 2017.

11. Azmi, R.; Tibben, W.; Win, K.T. Review of cybersecurity frameworks: Context and shared concepts. J. Cyber Policy 2018, 3, 258–283. [CrossRef]

12. Dawson, M. Hyper-connectivity: Intricacies of national and international cyber securities. In PQDT—Glob; London Metropolitan University: London, UK, 2017.

13. Lopes, I.M.; Guarda, T.; Oliveira, P. Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. J. Inf. Syst. Eng. Manag. 2019, 4, em0089. [CrossRef]

14. Cockcroft, S. What is the nist framework. ITNOW 2020, 62, 48–49. [CrossRef]

15. Ferruzola Gómez, E.; Duchimaza, S.J.; Ramos Holguín, J.; Alejandro Lindao, M. Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. Rev. Científica Tecnológica UPSE 2019, 6, 34–41. [CrossRef] 16. Popchev, I.; Radeva, I.; Nikolova, I. Aspects of the Evolution from Risk Management to Enterprise Global Risk Management. Eng. Sci. 2021, LVIII,

16–30. [CrossRef]

17. Ahmad, R.; Alsmadi, I. Machine learning approaches to IoT security: A systematic literature review[Formula presented]. Internet Things 2021, 14, 100365. [CrossRef]

18. Griffy-Brown, C.; Chun, M.; Lazarikos, D. Emerging Technologies and Cyber Risk: How do we secure the Internet of Things (IoT) environment? J. Appl. Bus. Econ. 2019, 21, 70–79. [CrossRef]

19. Falivene, L.; Tucker, B. Unifying Cyber Risk: Cyber Risk Maturity Model v1 Cyber Risk Maturity Model Construction Process & Maturity Model Document; Universidad de Buenos Aires: Buenos Aires, Argentina, 2021.

20. Tatiara, R.; Fajar, A.N.; Siregar, B.; Gunawan, W. Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001. In Proceedings of the Journal of Physics: Conference Series, Medan, Indonesia, 28–30 November 2018; Volume 978.

ISSN PRINT 2319 1775 Online 2320 787
 Journal Volume 10, Iss 08, 2021

21. Lambrinoudakis, C.; Gritzalis, S.; Xenakis, C.; Katsikas, S.; Karyda, M.; Tsochou, A.; Papadatos, K.; Rantos, K.; Pavlosoglou, Y.; Gasparinatos, S.; et al. Compendium of Risk Management Frameworks with Potential Interoperability: Supplement to the Interoperable EU Risk Management Framework Report; European Union Agency for Cybersecurity (ENISA): Athens, Greece, 2022; ISBN 9789292045548.

22. Tranfield, D.; Denyer, D.; Smart, P. Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. Br. J. Manag. 2003, 14, 207–222. [CrossRef]

23. Xiao, Y.; Watson, M. Guidance on Conducting a Systematic Literature Review. J. Plan. Educ. Res. 2019, 39, 93–112. [CrossRef]

24. Lame, G. Systematic literature reviews: An introduction. Proc. Int. Conf. Eng. Des. ICED 2019, 1, 1633–1642. [CrossRef]

25. Ali, R.F.; Dominic, P.D.D.; Ali, S.E.A.; Rehman, M.; Sohail, A. Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. Appl. Sci. 2021, 11, 3383. [CrossRef]