Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats

Juan Luis Salas-Riega[1], Yasmina Riega-Virú[2], Mario Ninaquispe-Soto[3], José Miguel Salas-Riega[4]
Pontificia Universidad Católica Del Perú, Lima, Perú[1, 4]
Universidad Privada Del Norte, Lima, Perú[2, 3]

***Abstract*—This systematic review evaluates the adoption and effectiveness of the NIST Cybersecurity Framework (CSF) in mitigating cyber threats across diverse sectors. Following PRISMA guidelines, we analyzed studies published between 2015 and 2024 from major academic databases, focusing on the framework's five core functions: Identify, Protect, Detect, Respond, and Recover. Results indicate widespread recognition but uneven adoption—large organizations show strong performance in the Protect and Detect functions, while small and medium-sized enterprises (SMEs) face implementation barriers due to limited resources. The framework's flexibility and risk-based approach are notable strengths, though its voluntary nature and lack of localized standards pose challenges. Compared to ISO/IEC 27001 and COBIT, NIST CSF is more adaptable but less prescriptive. We identify key gaps in empirical validation and sector-specific applications, and recommend future research integrating AI-driven threat detection and regional adaptations.**

***Keywords*—Cyberattacks; small and medium enterprises; risk management; organizational resilience; cyberthreats**

I. Introduction

Digital transformation has redefined human interaction and organizational operations. Unlike traditional physical spaces, cyberspace represents a unique communication realm that is essentially relational in nature, where virtual communities connect through shared interests rather than geographical proximity [1]. This digital domain has evolved into a comprehensive social, business, political, and economic ecosystem that transcends conventional boundaries. In Latin America, this transformation has been particularly profound, with cloud computing, mobile devices, and broadband networks enabling governments and businesses to make more integrated and effective decisions [2].

However, the rapid expansion of digital technologies has created a paradoxical situation. While these advances have simplified many aspects of daily life, they have simultaneously made opportunities for cybercrimes vast and inevitable [3]. The growth of cyberspace has dramatically increased the threats and challenges of cybersecurity, particularly in sectors like higher education, where various platforms enable constant interaction among students, faculty, and staff [4]. This highlights the urgent need for robust cybersecurity in an increasingly interconnected world.

Cybersecurity encompasses the comprehensive set of practices and technologies designed to protect data, devices, networks, and critical infrastructures from threats and attacks. Its primary focus lies in ensuring the confidentiality, integrity, and availability of digital systems and services [5]. This field extends beyond mere technological protection to include both physical and logical security of computer systems, with the ultimate objective of safeguarding information on digital media and the systems that house them [6]. Recent developments in information and communication technology have transformed the nature of threats---particularly in sectors like banking, where fraud has evolved significantly---the need for advanced prevention measures has become increasingly apparent [7].

The vulnerability of interconnected systems becomes particularly evident in critical infrastructure sectors. For instance, the maritime industry, which relies heavily on interconnected networks, communication systems, and sophisticated technologies, has become an attractive target for cybercriminals, nation-states, and other threat actors [8]. Similarly, healthcare systems face unprecedented risks, with ransomware attacks on healthcare provider information systems demonstrating the potential to impact patient mortality and morbidity [9]. These examples illustrate how cybersecurity concerns extend beyond data protection to encompass human welfare and the continuity of essential services.

The growing digitalization and technological dependence in Latin America have exposed governments and organizations to increasingly sophisticated cyber threats, including ransomware, hacktivism, and cyber espionage. These attacks have severely impacted critical sectors such as energy, health, and finance, compromising data confidentiality and the operability of essential services [10]. Despite adopting emerging technologies like blockchain and machine learning, the region faces significant limitations in integrating international regulatory frameworks like NIST and developing the technical capacity to prevent and respond to incidents effectively [9].

The evolution of cyber threats demonstrates remarkable creativity in exploiting technological and organizational vulnerabilities [9], [10]. Contemporary attacks range from traditional banking network intrusions to sophisticated Internet of Things (IoT) exploits and coordinated disinformation campaigns. These evolving threats demand equally sophisticated protection strategies that combine international cooperation, specialized training, and the implementation of

adaptable frameworks such as NIST, tailored explicitly to regional particularities [9].

In response to this complex threat landscape, the NIST Cybersecurity Framework (CSF) has emerged as a globally recognized tool for addressing cyber risks. Introduced in 2014 and subsequently updated to version 2.0, this framework provides an adaptable structure that helps organizations identify, protect, detect, respond, and recover from cyber threats [8]. The updated NIST Cybersecurity Framework 2.0 serves as a standardized guideline designed to support organizations across all levels---from management to IT staff---in implementing comprehensive cybersecurity management approaches [11].

The framework's flexibility allows for integration with other standards, as demonstrated by efforts to create evaluation frameworks that measure information security maturity by combining NIST CSF with COBIT 2019 [4]. However, despite its widespread adoption and proven adaptability, significant questions remain regarding its implementation effectiveness and measurable impact on threat prevention across diverse organizational contexts.

Fig. 1 illustrates the five core functions of the NIST Cybersecurity Framework—Identify, Protect, Detect, Respond, and Recover—organized in a continuous, cyclical process that supports risk-based cybersecurity management.

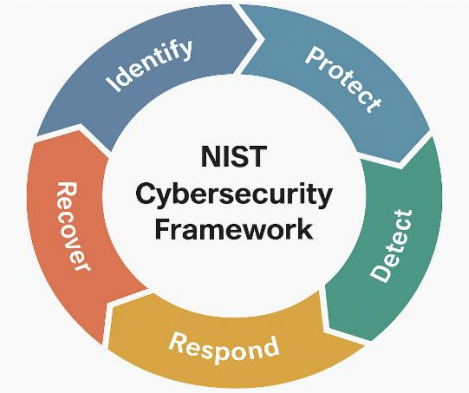

Fig. 1. NIST Cybersecurity framework: Core functions and their cyclical relationship. Adapted by the authors based on NIST (2018).

This systematic literature review addresses three fundamental research questions:

- What is the effectiveness of NIST Framework implementation in preventing cyber threats?
- How has the NIST Framework been implemented across different sectors and contexts?
- What observable impacts have resulted from its implementation?

The findings of this research will contribute to the existing body of knowledge regarding NIST Framework implementation and outcomes, while offering practical solutions and guidance for improving cybersecurity in diverse contexts. This is particularly relevant for Latin America, where limited resources, lack of expertise, and rapid technological advancements present critical barriers to effective security implementation [9]. This study aims to provide actionable insights to enhance cybersecurity resilience across the region and beyond by examining implementation patterns, effectiveness measures, and documented outcomes.

The remainder of this paper is organized as follows: Section II details the methodology and selection criteria used in the systematic review. It outlines the core components and operational principles of the NIST Cybersecurity Framework. Section III presents the main findings, emphasizing implementation outcomes and sector-specific trends. Discussion is given in Section IV. Section V and Section VI proposes directions for future research, and concludes with key insights and practical recommendations.

II. Materials and Methods

The systematic review followed the PRISMA framework [12], [13] and employed searches across four academic databases: Scopus, Web of Science, ProQuest, and ScienceDirect. Three complementary search strings were used to identify relevant studies between January 2020 and December 2024. Results were consolidated in Excel tables, applying temporal filters and inclusion and exclusion criteria and eliminating duplicates within and between databases to ensure a final set of unique and relevant articles. As shown in Table I, most studies were retrieved from Scopus, followed by Web of Science, ProQuest, and ScienceDirect.

In Scopus, two searches were performed using the defined strings. The first, "CSF OR NIST AND threats AND cybersecurity", generated 34 initial results, from which 21 articles were selected after applying temporal filters and excluding irrelevant ones. The second search, with the string ("NIST Cybersecurity Framework" OR "NIST CSF" OR "NIST Framework") AND ("information security" OR "risk management") NOT (medicine OR books OR news), generated 74 initial results, from which 59 articles were selected after filtering and reviewing abstracts. Then, duplicates were eliminated compared to the 21 articles from the first search, resulting in 19 additional articles. In total, Scopus contributed 40 unique articles.

TABLE I. Search Strings and Number of Articles Selected by Database

Search string	Scopus	Web of Science	ProQuest	ScienceDirect
CSF OR NITS AND threats and Cybersecurity	21	6	-	-
Implementation AND effectiveness AND csf 2.0 OR nits AND cybersecurity	-	-	4	-
("NIST Cybersecurity Framework" OR "NIST CSF" OR "NIST Framework") AND ("information security" OR "risk management") NOT (medicine OR books OR news)	19	-	-	4
Total = 54	40	6	4	4

In Web of Science, the string "CSF OR NIST AND threats AND cybersecurity" was used, obtaining 91,703 initial results. After applying filters that included only articles with the keyword "NIST", the results were reduced to 35. After applying temporal filters and reviewing abstracts, 23 relevant articles were selected. Compared with the 43 unique articles from Scopus, duplicates were identified, finally selecting 3 additional unique articles.

In ProQuest, the search with the string "Implementation AND effectiveness AND CSF 2.0 OR NIST AND cybersecurity" generated 17,939 initial results, which were reduced to 7,573 after applying a temporal filter. Subsequently, documents that did not correspond to scientific articles, conference proceedings, or systematic reviews were excluded, leaving 248 articles. Of these, only those with the keyword "NIST" in the title or abstract were selected, resulting in 10 articles. When compared with results from Scopus and Web of Science, 4 unique articles were selected.

In ScienceDirect, the string used was ("NIST Cybersecurity Framework" OR "NIST CSF" OR "NIST Framework") AND ("information security" OR "risk management") NOT (medicine OR books OR news), obtaining 138 initial results. After applying temporal filters, the results were reduced to 98. After excluding unrelated articles and reviewing abstracts, 10 relevant articles were selected. Finally, when compared with results from other databases, four unique articles were selected.

By integrating results from all databases and progressively eliminating duplicates, a total of 54 unique articles were obtained for this systematic review. This final set ensures the elimination of duplicates and ensures that all selected articles are relevant for the analysis.

III. Results

From the reading and analysis of the selected articles, the following results were obtained:

Fig. 2 displays the annual distribution of publications included in the review, with a notable increase in research activity from 2020 onward, suggesting a growing academic interest in the NIST Cybersecurity Framework in recent years.

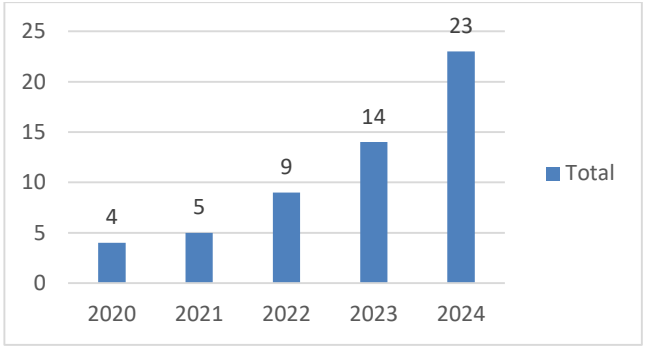

Fig. 2. Publications by year.

As shown in Fig. 3, the reviewed studies are concentrated in countries such as the United States, India, and the United Kingdom, indicating a higher level of research activity and documented implementation of the NIST Framework in these regions.

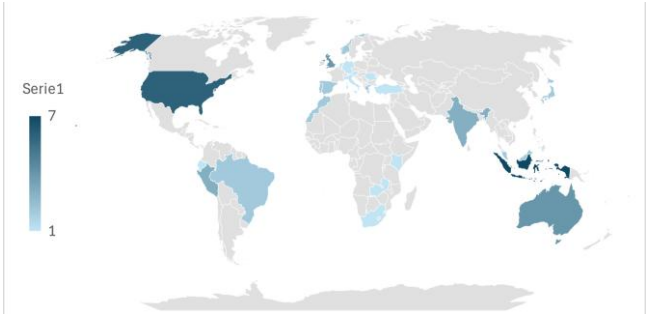

Fig. 3. Publications by country.

Note. Indonesia was identified as the country with the highest number of published articles, 7, followed by the United States with 6. In third place are Australia and the United Kingdom with 4 articles each. Peru and India contribute three articles each, while Brazil, Greece, Malaysia, Morocco, Norway, Portugal, and Spain contribute two articles each.

As shown in Table II, the selected studies span a wide range of sectors, including finance, healthcare, government, and critical infrastructure. The table also highlights the geographical distribution and publication dates of the analyzed works.

TABLE II. CSF Framework: Effectiveness, Methods, Purpose and Impacts on Cybersecurity

N	Authors	Effectiveness of NIST Framework implementation	NIST Framework implementation methods	Purpose of NIST Framework use in Cybersecurity	Observed impact on cyber threat prevention
1	[14] Lungu (2024)	x	x		x
2	[15] McIntosh et al. (2024)	x	x	x	
3	[16] Dimakopoulou and Rantos (2024)		x	x	x
4	[17] Hidayat and Wang (2023)	x	x	x	x
5	[18] Klien and Mohamed (2022)		x	x	
6	[19] Tissir et al. (2021)		x	x	
7	[20] El-Hajj and Mirza (2024	x	x	x	
8	[21] Torres et al. (2022)		x	x	
9	[22] Möller (2023)	x	x	x	x
10	[23] Kwon et al. (2020)		x	x	x
11	[24] Tan and Tan (2024)	x	x	x	
12	[25] Kannelonning and Katsikas (2024)	x	x	x	
13	[26] Yulianto et al. (2023)	x	x		
14	[27] Safitri and Kabetta (2023)	x	x		
15	[28] Lopes et al .(2024)		x	x	

16	[29] Amine et al. (2023)	x	x		
17	[30] Yulianto et al. (2023)	x			
18	[31] Muñoz et al. (2023)	x			
19	[32] Coppola et al. (2023)	x	x	x	x
20	[33] Kayashima et al. (2023)	x	x	x	x
21	[34] Botha-Badenhorst (2023)	x	x	x	
22	[35] Gourisetti et al. (2020)	x	x	x	x
23	[36] Benz and Chatterjee (2020)	x	x	x	x
24	[37] Ludin et al. (2024	x	x	x	
25	[38] Chidukwani et al. (2022)	x	x		x
26	[39] Progoulakis et al. (2024)	x	x	x	x
27	[40] Chidukwani et al. (2024)	x	x	x	
28	[41] Chourasia et al. (2024)	x	x	x	x
29	[42] Abergos and Medjek (2024)	x	x	x	x
30	[43] Lucchese et al. (2024)	x	x	x	x
31	[44] Domnik and Holland (2024)	x	x	x	x
32	[45] Santos et al. (2024)	x	x	x	x
33	[46] Maesschalck et al. (2022)	x	x	x	x
34	[47] Rosado et al. (2022)	x	x	x	x
35	[48] Soner et al. (2024)	x	x	x	x
36	[49] Marcel et al. (2024)	x	x		
37	[50] Salley et al. (2024)	x	x		
38	[51] Adriko and Nurse (2024)	x			
39	[52] Putro et al. (2024)	x			
40	[53] Falowo et al. (2023)	x	x		
41	[54] Hopcraft (2021)	x	x		
42	[55] Moreira et al. (2021)		x	x	
43	[56] Kaliappan et al. (2024)	x	x		
44	[57] Egan et al. (2020)	x	x		
45	[58] Gordon et al. (2020)		x	x	
46	[59] Azinheira et al. (2023)		x	x	
47	[60] Moturi et al. (2021)	x			
48	[61] Udroiu et al. (2022)			x	
49	[62] Perdana et al. (2022)				x
50	[63] Zarria et al. (2022)	x			
51	[64] Mukhopadhyay and Jai (2024)	x	x		
52	[65] De la Torre et al. (2024)	x	x		
53	[66] Evang (2023)	x	x		
54	[67] Torres-Calderon et al. (2022)	x			
		43	45	32	20

Table III summarizes the primary objectives and research contributions of each study, including case applications, comparative analyses, and proposals for implementation models of the NIST framework.

TABLE III. EFFECTIVENESS OF ITS IMPLEMENTATION

N	Authors	Reduction of cyberattacks	Effectiveness opinions by sector	Before and after comparison	Model proposals
1	Lungu (2024)	x			x
2	McIntosh, T et al (2024)		x	x	
3	Torres-Calderón et al. (2021)	x			
4	Angelo et al. (2024)	x			x
5	Progoulakis et al. (2024)	x			
6	Hidayat and Wang (2023)		x		
7	El-Hajj and Mirza (2024)		x		
8	De la Torre et al. (2024)		x		
9	Möller (2023)	x		x	
10	Tan & Tan (2024)		x		x
11	Kannelonning K.; Katsikas S (2024)	x			x
12	Yulianto, et al (2023)		x	x	
13	Safitri E.H.N.; Kabetta H (2023)		x	x	
14	Rosado et al. (2024)			x	
15	Coppola et al. (2024)			x	x
16	Safitri and Kabetta (2023)				x
17	Lucchese et al. (2024)	x			x
18	Gourisetti et al. (2024)	x			x
19	Putro et al. (2023)	x	x		x
20	Hopcraft R. (2023)		x		x
21	Moreira et al. (2024)		x		
22	Kaliappan et al. (2024)	x	x		
23	Benz & Chatterjee (2023)	x	x		
24	Maesschalck et al. (2023)		x	x	x

25	Ludin et al. (2023)	x			x
26	Chidukwani et al. (2023)	x			x
27	Soner et al. (2024)			x	x
28	Udroiu et al. (2024)	x	x		
29	Perdana et al. (2024)			x	x
30	Zarria et al. (2022)	x	x		
31	Mukhopadhyay & Jain (2024)		x		x
32	Santos et al. (2024)			x	
33	Torres-Calderón et al. (2024)			x	
34	Falowo et al. (2024)	x	x		x
35	De la Torre et al. (2024)		x		
36	Domnik & Holland (2023)				x
	Total	16	18	11	18

As illustrated in Table IV, the implementation of the NIST Framework is typically assessed along several dimensions, including technical tools, risk management strategies, organizational readiness, and policy alignment.

TABLE IV. NIST FRAMEWORK IMPLEMENTATION METHODS IN DIFFERENT CONTEXTS

N	Authors	Adopted methods	Tools and technologies used	Adaptations for implementation	Problems encountered
1	Lungu (2024)	x			x
2	Dimakopoulou and Rantos (2023)	x	x		x
3	Hidayat and Wang (2023)	x		x	
4	McIntosh et al. (2024)		x		
5	Coppola et al. (2024)		x		
6	Torres et al. (2024)		x		x
7	El-Hajj and Mirza (2024)			x	
8	Angelo et al. (2024)			x	
9	Lucchese et al. (2024)			x	
10	Chidukwani et al. (2024)				x
11	Rosado et al. (2024)				x

According to Table V, key challenges in adopting the NIST Framework include limited financial resources, lack of cybersecurity awareness, and difficulties in adapting the framework to specific contexts. The table also presents proposed solutions, such as training programs, toolkits, and phased implementation approaches:

TABLE V. PURPOSE OF NIST FRAMEWORK USE IN CYBERSECURITY

N	Autores	Implementation purpose	Specific use	Beneficiaries
1	Dimakopoulou et al. (2024)	x		
2	Hidayat and Wang (2023)	x		
3	Kayashima et al. (2024)	x		
4	Botha-Badenhorst (2023)	x		
5	McIntosh et al. (2024)		x	
6	El-Hajj and Mirza (2024)		x	
7	Coppola et al. (2024)		x	
8	Lucchese et al. (2024)		x	
9	Torres et al. (2024)			x
10	Santos et al. (2023)	x		x
11	Benz and Chatterjee (2023)			x
12	Chourasia et al. (2024)			x

Observed impacts on cyber threat prevention have emerged as a central theme in the selected studies, reflecting the practical effectiveness of the NIST Cybersecurity Framework (CSF) across various sectors. As documented in Table VI, the reviewed literature reports three major categories of impact: (1) observable changes in cyber threat behavior or system vulnerabilities, (2) increased recovery capacity following cyber incidents, and (3) strengthened governance and risk management practices. These findings indicate that the implementation of the NIST CSF not only enhances preventive mechanisms but also contributes to resilience during and after incidents. Notably, improvements in recovery capacity and governance were frequently associated with adaptations of the framework to sector-specific needs, particularly in critical infrastructure and SMEs. The observed changes further suggest that the NIST CSF's modularity allows for scalable and contextualized applications, supporting more strategic cybersecurity planning. The following table summarizes the studies that reported impacts in at least one of these three categories.

Table VI categorizes the reported impacts of NIST implementation into three main areas: reduction of vulnerabilities, improved incident response and recovery capacity, and enhanced cybersecurity governance structures.

TABLE VI. OBSERVED IMPACT ON CYBER THREAT PREVENTION

N	Authors	Observed changes	Increase in recovery capacity	Improvements in governance and risk management
1	Dimakopoulou et al. (2024)	x	x	
2	Hidayat and Wang (2023)	x	x	x
3	Möller (2023)	x	x	x
4	Kwon et al. (2024)	x	x	x
5	Coppola et al. (2024)	x	x	x
6	Kayashima et al. (2024)	x	x	
7	Gourisetti et al. (2024)	x	x	x
8	Benz and Chatterjee (2023)	x	x	x
9	Chourasia et al. (2024)	x		x
10	Lucchese et al. (2024)	x	x	
11	Rosado et al. (2024)	x	x	x

Fig. 4. NIST, "Spanish translation of the NIST cybersecurity framework 2.0," 2024.

Fig. 4 illustrates that the recently released NIST Cybersecurity Framework 2.0 introduces notable enhancements that align with the evolving threat landscape. It reinforces its outcome-based orientation, allowing organizations to tailor cybersecurity objectives to specific risk profiles. Governance is now positioned as a cross-cutting theme within the Identify function, reflecting its foundational role in ensuring security across all operational domains. Furthermore, the framework emphasizes the integration of cybersecurity with enterprise risk management (ERM), the inclusion of supply chain risk considerations, and expanded tools such as sector-specific profiles and quick-start guides to support implementation in SMEs. These updates respond to the growing demand for adaptable yet actionable frameworks across diverse sectors and geographies [68].

IV. Discussion

A. Effectiveness of NIST Framework Implementation

The present systematic review allowed us to analyze the effectiveness of the NIST framework implementation across diverse contexts, considering key aspects such as cyberattack reduction, sector-specific effectiveness perspectives, pre- and post-implementation comparisons, and proposals for derivative models. The following discussion explores the most significant findings:

1) Reduction of cyberattacks: The reviewed studies demonstrate a consensus regarding the effectiveness of the NIST Cybersecurity Framework (CSF 2.0) in reducing cyberattacks, although approaches and results vary considerably across sectors and contexts. Torres-Calderón et al. [67] and Angelo et al. [69] provided robust evidence that structured implementation of framework controls significantly improves organizational cybersecurity posture, achieving increases ranging from 40% to 55.6% in cyber maturity within SMEs and organizations in Peru. Nevertheless, these studies also underscore that improvements are contingent upon resource availability and organizational capacity to adapt the framework to local requirements. This raises a critical question: can the framework demonstrate equal effectiveness in contexts characterized by limited capabilities?

Within the industrial sphere, Progoulakis et al. [39] and Gourisetti et al. [35] argue that the framework's effectiveness stems from its capacity to prioritize critical controls and enable network segmentation, which proves particularly valuable in cyber-physical systems such as maritime infrastructures and vital installations. However, these proposals encounter significant challenges in sectors where implementing advanced technologies, including artificial intelligence and real-time monitoring systems, remains constrained. Putro et al. [52] expand this discussion by suggesting that integrating specific tools may be pivotal for practical CSF application in government systems, where risks are frequently associated with misconfigurations and governance deficiencies.

Conversely, financial and medical sectors present cases where the framework demonstrates greater effectiveness when focused on fundamental controls. Ludin et al. [37] and Chidukwani et al. [38] highlight that practices such as access control policies and continuous monitoring have enabled technological SMEs to mitigate common threats, including phishing and ransomware attacks. Similarly, Udroiu et al. [61] argue that encryption and advanced authentication strategies strengthen cyber resilience in medical systems when aligned with the CSF. However, these applications illustrate a tendency to prioritize preventive functions, while response and recovery capabilities often remain underdeveloped, a challenge explicitly noted by Benz & Chatterjee [36].

Finally, studies by Falowo et al. [53] and Safitri & Kabetta [27] demonstrate the framework's utility in mitigating advanced threats such as ransomware through controls adapted to organizational requirements. These findings align with Zarria et al. [63], who indicate that risk governance, when supported by the NIST CSF, experiences significant enhancement. However, the discussion suggests that although the framework exhibits high adaptability, its success remains dependent on strategic implementation and each sector's capacity to overcome operational and technical barriers.

2) Effectiveness opinions by sector: Analysis of CSF effectiveness across different sectors reveals its adaptability and inherent limitations. In the financial industry, Hidayat and Wang [17] and Zarria et al. [63] emphasize that the framework strengthens governance and enables investment prioritization, which proves crucial in institutions where cyber risk can generate significant economic repercussions. However, Benz & Chatterjee [36] and El-Hajj and Mirza [20] note that while the framework facilitates risk mitigation in resource-limited sectors, its implementation frequently encounters obstacles due to lack of empirical analyses and simplified tools adapted to these contexts.

In the educational sector, De la Torre et al. [65] and Santos et al. [45] demonstrate that the CSF can be adapted to address specific vulnerabilities, such as unauthorized access and weak passwords, through simulations and risk assessments. However, these strategies also reveal a dependence on technical and human resources that are not consistently available, particularly in environments with budgetary constraints. This reality underscores the need to simplify

framework implementation to enhance accessibility in sectors where structural limitations constitute critical barriers.

In industry, Kannelønning and Katsikas [25] identified a significant gap between the perceived importance of controls and their actual implementation in Norway's Industry 4.0, evidencing a common challenge: insufficient training and resources dedicated to operational cybersecurity. Meanwhile, Maesschalck et al. [46] and Chidukwani et al. [38] highlight that partial CSF adoption in manufacturing and services has successfully improved cyber resilience, particularly when addressing specific threats through technological maturity solutions. However, this progress remains conditional upon organizations' ability to integrate the framework with customized approaches that address sector-specific complexities.

Governance and cyber resilience have also benefited from specific exercises aligned with the CSF, as demonstrated by Yulianto et al. [30] and Falowo et al. [53]. These studies emphasize how practices such as Red Teaming and risk planning improve threat detection and response and enhance organizational awareness of vulnerabilities. In a governmental context, Putro et al. [52] emphasize that tools adapted to the framework have enabled risk mitigation in administrative services, while Moreira et al. [55] indicate that CSF effectiveness in the energy sector depends significantly on overcoming technological and operational barriers.

In the maritime sector, Hopcraft [54] proposes that strengthening digital competencies aligned with the CSF reduces human errors, one of this industry's most prevalent attack vectors. This approach reinforces preparedness against cyberattacks and illustrates the necessity of combining technical framework implementation with human capacity development.

3) Comparison of before and after implementation: CSF implementation demonstrates a clear trend toward improving organizational cybersecurity; however, findings reveal that sectoral context, available resources, and customization level profoundly influence its effectiveness. Möller [22] and Rosado et al. [47] demonstrate that the framework can significantly reduce specific threats, such as phishing and breaches in hospital environments, when complemented with additional standards, including MITRE criteria and the MARISMA-CPS pattern. This approach suggests that the CSF, while effective, is not self-sufficient and requires specific adaptations to address critical sector complexities.

Furthermore, Coppola et al. [32] and McIntosh et al. [15] emphasize that sustained cybersecurity improvement depends on implementing initial controls and maintaining continuous framework evaluation against emerging threats. This raises a crucial consideration: are organizations adopting the CSF as an iterative process or perceiving it as a static model? This gap in understanding dynamic CSF utilization highlights the need for sector-specific guidelines that promote continuous evaluation and improvement cycles.

Ludin et al. [37] and Maesschalck et al. [46] document tangible improvements in cyber maturity when implementing basic CSF controls in resource-limited sectors such as SMEs. However, these improvements often lack long-term sustainability due to funding constraints and specialized personnel shortages. This challenge underscores the importance of simplifying the framework to enhance accessibility for organizations with limited capabilities. Despite these limitations, studies such as those by Safitri & Kabetta [27] demonstrate the feasibility of designing practical adaptations that integrate specific controls and risk planning in low-resource environments.

In the educational sector, Santos et al. [45] and Perdana et al. [62] highlight how the framework enables not only risk mitigation in academic systems but also the establishment of a structured foundation for anticipating future threats. However, these cases also reveal dependence on advanced tools and simulation practices, which limit applicability in institutions with budgetary restrictions. This finding raises a critical gap: how can the CSF be redesigned to balance technical sophistication with operational accessibility?

Finally, studies by Torres-Calderón et al. [67] and Safitri & Kabetta [27] provide quantifiable evidence regarding benefits of structured CSF-based approaches, such as the 55.6% increase in cybersecurity posture achieved by a Peruvian organization. These cases confirm the framework's effectiveness and highlight its potential for adaptation to specific contexts. However, they also suggest that CSF success depends on committed organizational leadership and long-term strategic vision.

These findings collectively contribute to understanding CSF effectiveness by revealing that while it represents a versatile tool, its impact depends on integration with sectoral practices, maintaining an iterative approach, and resolving structural barriers. This analysis not only confirms its value in global cybersecurity but also identifies key areas for future research, including simplification needs for vulnerable sectors and methodology design, ensuring sustainable application.

4) Model proposals: A recurring characteristic in the reviewed studies is the effort to adapt and complement the NIST CSF for specific contexts, highlighting its flexibility and utility while exposing limitations that justify new proposals. Lungu [14] and Coppola et al. [32] emphasize the importance of specialized models incorporating advanced technologies such as artificial intelligence and real-time monitoring, necessary for addressing technical challenges in systems including GPUs and cloud services. These proposals respond to the need for confronting emerging threats, such as configuration errors and hardware vulnerabilities, demonstrating that the CSF can provide a solid foundation when expanded to cover these areas.

Conversely, resource-limited sectors also benefit from adapted models. Angelo et al. [690] and Safitri & Kabetta [27] proposed frameworks integrating continuous improvement (PDCA) and specific controls for technological risks. These initiatives reflect how the NIST CSF can be optimized for small or medium organizations, particularly those with limited financial and human resources. Similarly, Perdana et al. [62]

and De la Torre et al. [65] emphasize that adaptations in educational and academic environments strengthen cyber resilience and enable proactive risk management in critical systems.

The industrial sector has also discovered opportunities for CSF customization. Maesschalck et al. [46] and Soner et al. [48] propose combined strategies integrating traditional risk assessment methodologies with specific solutions for critical industrial networks. This approach complements findings by Domnik & Holland [44], who address data protection maturity, and Hopcraft [54], who highlights the need for hierarchical models of digital competencies to enhance cybersecurity in maritime sectors.

Finally, model proposals also reflect consensus regarding strengthening governance and organizational resilience. Yulianto et al. [26] and Chidukwani et al. [38] highlight how implementing Red Teaming exercises and simplified methodologies can transform response and detection capabilities in industrial and service sectors. These initiatives not only address specific weaknesses but also demonstrate how the CSF can serve as a foundational framework for developing more dynamic strategies.

B. NIST Framework Implementation Methods

1) Adopted methods: The methods adopted for NIST CSF implementation vary significantly according to context and sector-specific needs. Lungu [14] describe the utilization of hardware performance counters and defense techniques against side channels to protect heterogeneous architectures in high-performance environments. This approach highlights the framework's versatility in adapting to technologically advanced contexts.

In the maritime domain, Dimakopoulou and Rantos [16] emphasize the implementation of anomaly detection technologies and continuous monitoring, enabling the addressing of specific challenges such as system interoperability in maritime supply chains. Meanwhile, in non-banking financial systems, Hidayat and Wang [17] propose a maturity model based on the five NIST CSF functions, prioritizing detection and recovery to strengthen cyber resilience.

2) Tools and technologies used: The deployment of tools and technologies in NIST CSF implementation demonstrates an adaptive and efficient approach. McIntosh et al. [15] discussed integrating automated processes, continuous audits, and human validation to manage risks associated with language models. Similarly, Coppola et al. [32] describe applying advanced services such as AWS GuardDuty and Security Hub, along with machine learning models, to mitigate cloud risks.

In the educational sector, Torres et al. [67] developed a React and .NET-based tool to assess NIST CSF compliance, enabling schools to identify critical gaps and customize improvement plans. This approach demonstrates how specific technologies can be adapted to sectors with limited resources.

3) Adaptations for implementation: The adaptations implemented for the NIST CSF reflect the necessity of customizing its functions according to specific sector demands. El-Hajj and Mirza [20] adjusted framework controls to establish security levels, allowing small and medium enterprises (SMEs) to adopt progressive measures aligned with their capabilities. Similarly, Angelo et al. [69] designed a hybrid framework combining the Deming cycle (PDCA) with NIST CSF controls, optimizing applicability in Peruvian SMEs.

In the cyber-physical systems industry, Lucchese et al. [43] introduced digital twins for real-time monitoring and anomaly detection, improving threat identification accuracy in critical systems such as manufacturing. This model highlights the NIST CSF's capacity to integrate with advanced technologies and address emerging challenges.

4) Problems encountered during implementation: Despite its benefits, NIST CSF implementation faces several significant challenges. Lungu [14] identified system performance compromises resulting from integrating advanced defense techniques. Similarly, Dimakopoulou and Rantos [16] noted the absence of specific guidelines for addressing complex risks such as attacks on GNSS and AIS systems in the maritime sector.

In the educational sector, Torres et al. [21] highlighted framework complexity and resource limitations as significant barriers to implementation in K-12 schools. Likewise, Chidukwani et al. [40] emphasized that SMEs face financial and technical expertise constraints, which complicate full framework adoption.

Finally, Rosado et al. [47] documented initial complexity in configuring patterns such as MARISMA-CPS, emphasizing the need for risk analysis experts to customize the framework for critical sectors such as healthcare.

C. Purpose of NIST Framework Use in Cybersecurity

The systematic review identified that the NIST Framework is implemented primarily to address three major objectives: critical infrastructure protection, regulatory compliance, and organizational resilience enhancement. Dimakopoulou et al. highlighted the importance of protecting critical infrastructures in the maritime sector, specifically addressing threats related to supply chains and autonomous systems [16]. Similarly, Hidayat and Wang emphasized cyber resilience improvement and regulatory compliance in non-banking financial institutions, reinforcing governance and sensitive data protection [17].

Implementation purposes respond to concrete requirements in specific sectors. Kayashima et al. addressed critical vehicular system protection, focusing on vehicular networks and V2X communication [33]. Meanwhile, Botha-Badenhorst emphasized how the framework balances innovation and cybersecurity in technology industries, ensuring innovative asset protection [34].

1) Specific use: The specific NIST Framework applications identified in reviewed studies range from cloud security to the detection and mitigation of advanced threats. McIntosh et al. integrated the NIST CSF with other frameworks, such as ISO 42001, to protect AI applications, including Large Language Models (LLMs), ensuring real-time analysis and cloud security [15]. Similarly, El-Hajj and Mirza developed tools to mitigate threats such as phishing and malware, adapting framework controls for small and medium enterprises [20].

A relevant case of framework customization is the study by Coppola et al., who deployed the NIST CSF in AWS environments to prevent unauthorized access and protect critical cloud configurations [32]. Additionally, Lucchese et al. proposed digital twin utilization in critical industrial systems, demonstrating how the framework facilitates cyber-physical attack detection through real-time monitoring [43].

2) Beneficiaries: The beneficiaries identified in reviewed studies vary according to implementation context but include governmental, industrial, educational, and service sectors. Torres et al. developed a self-assessment tool for Australian K-12 schools, directly benefiting students, teachers, and administrative staff [21]. In the energy sector, Santos et al. applied the NIST CSF in photovoltaic systems to protect critical infrastructure and ensure operational continuity, benefiting both operators and end users [45].

The focus on small and medium enterprises (SMEs) is particularly relevant. Benz and Chatterjee introduced a simplified assessment tool that enables SMEs to improve their cybersecurity posture without requiring substantial technical or financial resources, thus strengthening their resilience against cyberattacks [36]. Similarly, Chourasia et al. highlighted that small businesses can benefit from simplifying NIST CSF functions to address limited resources and technical skill deficiencies [41].

D. Observed Impact on Cyber Threat Prevention

This section analyzes the implications of findings reflected in Table V, highlighting observed changes, increases in recovery capacity, and improvements in governance and risk management resulting from NIST CSF Framework implementation across various contexts.

1) Observed changes: The systematic review results demonstrate that relevant studies report significant improvements in cyber resilience. Dimakopoulou and Rantos observed advances in critical maritime system protection, highlighting the capacity to mitigate cyberattacks in port operations through continuous monitoring and early anomaly detection [16]. This underscores how the NIST Framework can effectively adapt to specific sectors, increasing its relevance in the maritime industry.

In the case of Coppola, Varde, and Shang, changes focused on correcting misconfigurations in cloud platforms, resulting in improved early detection of critical vulnerabilities [32]. This reinforces that precise identification of technical problems is fundamental for ensuring security in highly dynamic environments.

Meanwhile, Lucchese, Salerno, and Pugliese achieved significant advances in early cyberattack detection through the utilization of digital twins in industrial systems [43]. This underscores the potential of combining emerging technologies with NIST Framework principles to address complex threats.

2) Increase in recovery capacity: Recovery capacity following incidents was a comprehensively documented dimension. According to Möller, the implementation of NIST CSF controls, complemented with MITRE criteria, facilitated faster recovery of critical systems affected by cyberattacks [22]. This approach highlights how framework combination can offer more robust strategies for addressing cyber threats.

Additionally, the study by Kayashima et al. identified restoration strategies based on validated monitoring points, which enabled incident mitigation before escalation to critical levels [33]. This evidence emphasizes the importance of implementing preventive controls in sectors such as the automotive industry, where connectivity plays a crucial role.

Gourisetti et al. emphasized how gap prioritization through the CyFEr methodology helped restore system maturity affected by attacks [35]. Automation and elimination of human biases in control prioritization are key factors for strengthening operational resilience.

3) Improvements in governance and risk management: Governance and risk management were central aspects in the reviewed studies. Benz and Chatterjee's work demonstrated how small and medium enterprises (SMEs) can prioritize critical controls to optimize limited resource management [36]. The CET tool improves cyber posture and provides a practical framework for guiding strategic security decisions.

Furthermore, analysis by Santos et al. in cyber-physical photovoltaic systems indicated that integrating standards such as the NIST CSF with specific methods strengthened strategic decision-making and optimized risk management in critical infrastructures [45]. This highlights the necessity for adapted sectoral approaches to address unique vulnerabilities.

Finally, the study by Maesschalck et al. on honeypot utilization within industrial systems emphasizes how collected data can inform organizational policies and strategic decisions, improving preparedness against cyber threats [46].

E. Comparison with Other Cybersecurity Frameworks

Table VII introduces a side-by-side comparison of the three most widely cited cybersecurity frameworks—NIST CSF, ISO/IEC 27001, and COBIT 2019—to clarify how each one serves a distinct strategic purpose. The NIST CSF delivers a voluntary, function-oriented roadmap that organizations can scale and reorder to match their individual risk appetites. ISO/IEC 27001, by contrast, mandates a certifiable information-security management system (ISMS) with rigorously prescribed controls—an asset for entities that must demonstrate third-party compliance. COBIT 2019 extends the lens still further, embedding cybersecurity within an enterprise-

wide IT-governance paradigm and aligning security outcomes with overall business value. Although the NIST CSF offers the greatest configurability, its non-prescriptive nature can yield inconsistent implementations; ISO/IEC 27001 ensures uniformity but at higher cost and complexity; and COBIT adds strategic breadth yet assumes a mature governance structure. Table VII distils these trade-offs, enabling decision-makers to select—or blend—the framework(s) best suited to their regulatory, operational, and resource realities.

TABLE VII. COMPARISON OF CYBERSECURITY FRAMEWORKS

Feature	NIST Cybersecurity Framework	ISO/IEC 27001	COBIT 2019
Primary Objective	Manage cyber risks using functional categories.	Establish a certifiable ISMS based on security controls.	Provide governance and management of enterprise IT.
Approach Type	Voluntary and flexible	Prescriptive, formal, and certifiable	Governance and process-based control model
Scope of Application	Cybersecurity specifically	General information security	Enterprise-wide IT, including cybersecurity
Level of Detail	High-level framework with profiles and categories	Detailed controls and annexed specifications	Highly detailed with governance components
Certification Available	No	Yes	No (supports audit but not certifiable by itself)
Suitability for SMEs	High, due to modularity and low cost	Low, due to complexity and certification costs	Medium, suited for mid-sized enterprises
Compatibility with Other Standards	Compatible with ISO, COBIT, CIS Controls	Compatible with NIST and other standards	Compatible with NIST and ISO
Suggested Citation	NIST, 2018	ISO, 2013	ISACA, 2019

Table VII presents a comparative analysis of the NIST Cybersecurity Framework, ISO/IEC 27001, and COBIT 2019, focusing on key differences in scope, certification, and suitability for SMEs.

V. FUTURE WORK

Future research should focus on empirical validation of the NIST framework across specific industries, particularly in SMEs and public sector organizations where implementation has been inconsistent. Additional studies could examine the integration of the framework with artificial intelligence and machine learning tools for real-time threat detection. Moreover, comparative studies evaluating the cost-benefit relationship between NIST and other frameworks (such as ISO/IEC 27001 or CIS Controls) would help determine the most suitable model for different organizational contexts. Finally, localized versions of the NIST framework adapted to regional cybersecurity regulations should be explored to enhance adoption in developing countries.

VI. CONCLUSION

The NIST Cybersecurity Framework (CSF) has significantly reduced cyberattacks, particularly within critical sectors including industry, healthcare, and SMEs. Implementation of the framework has yielded substantial improvements in cybersecurity maturity, with documented increases reaching up to 55.6% in certain cases. However, the framework's effectiveness varies considerably depending on resource availability and organizational capacity to adapt the framework to local requirements, highlighting the critical importance of customized approaches for each sector. The success of framework implementation remains contingent upon strategic deployment and sector-specific adaptations to overcome operational and technical barriers.

Implementation methods of the NIST Framework exhibit substantial variability across different contexts and sectors. Advanced sectors demonstrate sophisticated approaches utilizing technologies such as real-time monitoring and digital twins, while resource-constrained environments typically adopt progressive controls and adaptive tools. Despite documented benefits, significant challenges persist, including insufficient trained personnel and technical complexity of the framework, which particularly limit adoption in sectors such as education and SMEs. These findings underscore the necessity for framework simplifications that maintain effectiveness while enhancing accessibility for organizations with limited resources.

The primary purposes of the NIST Framework encompass critical infrastructure protection, regulatory compliance, and organizational resilience enhancement. The framework's specific applications range from cloud security to the protection of educational and vehicular systems, demonstrating its versatility across diverse sectors. Key beneficiaries include governments, enterprises, and academic institutions, all of which have successfully strengthened their cybersecurity postures and ensured operational continuity through framework-adapted tools. Small and medium enterprises have particularly benefited from simplified assessment tools that enable cybersecurity improvements without requiring substantial technical or financial resources.

The observable impact of the NIST Framework implementation is reflected in significant improvements across three key dimensions: early threat detection, enhanced recovery capacity, and strengthened governance and risk management. Integration of the framework with sector-specific standards has optimized resource allocation and improved strategic decision-making capabilities. While the framework demonstrates remarkable effectiveness, its ultimate success depends critically on strategic adaptations, committed organizational leadership, and technical and operational barriers resolution. This is particularly relevant in regions facing structural limitations, where simplified implementations and context-specific adaptations become essential for achieving sustainable cybersecurity improvements.

REFERENCES

[1] F. Miró, Cibercrimen Fenomenología y criminología de la delincuencia en el ciberespacio. Marcial Ponds Ediciones Jurídicas y Sociales, 2012.

[2] P. V. Villarreal, Inclusión digital y gobernanza de contenidos en internet. Reyno de los Países Bajos: Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, 2024. Accessed: Jun. 24, 2025. [Online]. Available: https://www.oas.org/es/cidh/expresion/informes/Inclusion_digital_esp.pdf

[3] M. Fadya and D. N. Utama, "Towards Secure Information Systems: Developing and Implementing an Information Security Evaluation Model Using NIST CSF and COBIT 2019," TEM Journal, pp. 182–191, Feb. 2025, doi: 10.18421/TEM141-17.

[4] M. A. Khan, A. A. Almulhim, and S. S. Alkati, "Towards the evaluation of cybersecurity threats and challenges in higher education institutions in Saudi Arabia," Edelweiss Applied Science and Technology, vol. 9, no. 2, pp. 657–669, 2025, doi: 10.55214/25768484.v9i2.4564.

[5] I. Conal, Ciberseguridad y Derecho Penal, Primera. España: Aranzadi, 2022.

[6] B. Bermejo and G. Atienza, Ciberseguridad, ciberespacio y ciberdelincuencia. Aranzadi Thomson Reuters, 2018.

[7] E. Tariq et al., "How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks," International Journal of Data and Network Science, vol. 8, no. 1, pp. 69–76, 2024, doi: 10.5267/j.ijdns.2023.10.016

[8] J. Pöyhönen, "Assessment of Cyber Security risks: A Smart Terminal Process," European Conference on Cyber Warfare and Security, vol. 22, no. 1, pp. 366–373, Jun. 2023, doi: 10.34190/eccws.22.1.1060.

[9] J. M. Aguilar Antonio, "La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas," Revista de Estudios en Seguridad Internacional, vol. 6, no. 2, pp. 17–43, Dec. 2020, doi: 10.18847/1.12.2.

[10] M. R. Cando-Segovia and P. Medina-Chicaiza, "Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica," 3C TIC: Cuadernos de desarrollo aplicados a las TIC, vol. 10, no. 1, pp. 17–41, Mar. 2021, doi: 10.17993/3ctic.2021.101.17-41.

[11] T. Olaes, "What is NIST Cybersecurity Framework (CSF) 2.0? | Balbix." Accessed: Jun. 25, 2025. [Online]. Available: https://www.balbix.com/insights/nist-cybersecurity-framework/.

[12] M. J. Page et al., "PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews," BMJ, p. n160, Mar. 2021, doi: 10.1136/bmj.n160.

[13] A. Ciapponi, "La declaración PRISMA 2020: una guía actualizada para reportar revisiones sistemáticas," Evidencia, actualizacion en la práctica ambulatoria, vol. 24, no. 3, p. e002139, Aug. 2021, doi: 10.51987/evidencia.v24i4.6960.

[14] N. Lungu, "NIST CSF-2.0 Compliant GPU Shader Execution", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15187–15193, Aug. 2024.

[15] T. McIntosh et al., "From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models," Comput Secur, vol. 144, p. 103964, Sep. 2024, doi: 10.1016/j.cose.2024.103964.

[16] A. Dimakopoulou and K. Rantos, "Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0," J Mar Sci Eng, vol. 12, no. 6, 2024, doi: 10.3390/jmse12060919.

[17] Hidayat V and Wang G, "A Comprehensive Cybersecurity Maturity Study for Nonbank Financial Institution," Journal of System and Management Sciences, vol. 13, no. 5, Sep. 2023, doi: 10.33168/JSMS.2023.0534.

[18] A. Klien and A. Mohamed, "Cybersecurity Intrusion Detection for Station and Process Bus Applications in Substations: Challenges and Experiences," in 2022 Saudi Arabia Smart Grid (SASG), IEEE, Dec. 2022, pp. 1–5. doi: 10.1109/SASG57022.2022.10199351.

[19] N. Tissir, S. El Kafhali, and N. Aboutabit, "Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal," J Reliab Intell Environ, vol. 7, no. 2, pp. 69–84, Jun. 2021, doi: 10.1007/s40860-020-00115-0.

[20] M. El-Hajj and Z. A. Mirza, "ProtectingSmall and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool," Electronics (Basel), vol. 13, no. 19, p. 3910, Oct. 2024, doi: 10.3390/electronics13193910.

[21] M. Torres, A. Mullins, and N. Thompson, "Education Cybersecurity Assessment Tool: A cybersecurity self-assessment tool for the Australian K-12 sector," ACIS 2022 Proceedings, Dec. 2022, Accessed: Jan. 18, 2025. [Online]. Available: https://aisel.aisnet.org/acis2022/96

[22] D. P. F. Möller, "NIST Cybersecurity Framework and MITRE Cybersecurity Criteria," in Guide to Cybersecurity in Digital Transformation, 2023, pp. 231–271. doi: 10.1007/978-3-031-26845-8_5.

[23] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, and S. N. Gupta Gourisetti, "Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping," in 2020 Resilience Week (RWS), IEEE, Oct. 2020, pp. 106–112. doi: 10.1109/RWS50334.2020.9241271.

[24] T. H. Tan and T. K. Tan, "E-Banking SAF: A TOGAF-NIST Aligned Security Architecture Framework for E-Banking Systems," in 2024 7th International Conference on Information and Computer Technologies (ICICT), IEEE, Mar. 2024, pp. 1–6. doi: 10.1109/ICICT62343.2024.00007.

[25] K. Kannelønning and S. Katsikas, "Deployment of Cybersecurity Controls in the Norwegian Industry 4.0," in Proceedings of the 19th International Conference on Availability, Reliability and Security, New York, NY, USA: ACM, Jul. 2024, pp. 1–8. doi: 10.1145/3664476.3670896.

[26] S. Yulianto, F. L. Gaol, S. Supangkat, and B. Ranti, "A Comprehensive Model for Enhancing Cybersecurity Resilience and IT Governance Through Red Teaming Exercises," in 2023 29th International Conference on Telecommunications (ICT), IEEE, Nov. 2023, pp. 1–7. doi: 10.1109/ICT60153.2023.10374068.

[27] E. Safitri and H. Kabetta, "Cyber-Risk Management Planning Using NIST CSF V1.1, ISO/IEC 27005:2018, and NIST SP 800-53 Revision 5 (A Study Case to ABC Organization)," in 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), IEEE, Aug. 2023, pp. 332–338. doi: 10.1109/ICoCICs58778.2023.10277652.

[28] S. Lopes, P. Leite, S. Carvalho, and P. Teixeira, "Using ITIL as part of the NIST Cybersecurity Framework," in 2024 12th International Symposium on Digital Forensics and Security (ISDFS), IEEE, Apr. 2024, pp. 1–6. doi: 10.1109/ISDFS60797.2024.10527256.

[29] A. Amine, E. Chakir, T. Issam, and Y. I. Khamlichi, "A Review of Cybersecurity Management Standards Applied in Higher Education Institutions," International Journal of Safety and Security Engineering, vol. 13, no. 6, pp. 1109–1116, Dec. 2023, doi: 10.18280/ijsse.130614.

[30] S. Yulianto, E. Krisnanik, and M. S. Hartawan, "Strengthening IT Governance in the Crypto Marketplace: Leveraging Penetration Testing and Standards Alignment," in 2023 International Conference on Informatics, Multimedia, Cyber and Informations System (ICIMCIS), IEEE, Nov. 2023, pp. 200–205. doi: 10.1109/ICIMCIS60089.2023.10349052.

[31] A. Muñoz, A. Palomino, and L. Wong, "Cybersecurity framework for SMEs in Peru based on ISO/IEC 27001 and CSF NIST controls," in 2023 18th Iberian Conference on Information Systems and Technologies (CISTI), IEEE, Jun. 2023, pp. 1–7. doi: 10.23919/CISTI58278.2023.10211874.

[32] G. Coppola, A. S. Varde, and J. Shang, "Enhancing Cloud Security Posture for Ubiquitous Data Access with a Cybersecurity Framework Based Management Tool," in 2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), IEEE, Oct. 2023, pp. 0590–0594. doi: 10.1109/UEMCON59035.2023.10316003.

[33] M. Kayashima, N. Kawaguchi, K. Ideguchi, and N. Morita, "An Extraction and Validity Evaluation Method Proposal for Monitoring Points for In-Vehicle Systems: Deriving Cybersecurity Requirements," IEEE Vehicular Technology Magazine, vol. 18, no. 2, pp. 80–88, Jun. 2023, doi: 10.1109/MVT.2022.3219239.

[34] D. Botha-Badenhorst, "Navigating the Intersection of Innovation and Cybersecurity: A Framework," European Conference on Research

Methodology for Business and Management Studies, vol. 22, no. 1, pp. 18–25, Aug. 2023, doi: 10.34190/ecrm.22.1.1490.

[35] S. N. G. Gourisetti, M. Mylrea, and H. Patangia, "Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis," Future Generation Computer Systems, vol. 105, pp. 410–431, Apr. 2020, doi: 10.1016/j.future.2019.12.018.

[36] M. Benz and D. Chatterjee, "Calculated risk? A cybersecurity evaluation tool for SMEs," Bus Horiz, vol. 63, no. 4, pp. 531–540, Jul. 2020, doi: 10.1016/j.bushor.2020.03.010.

[37] W. Ludin, M. Mohd, and W. Fariza, "Comparative Analysis of Small and Medium-Sized Enterprises Cybersecurity Program Assessment Model," International Journal of Advanced Computer Science and Applications, vol. 15, no. 8, 2024, Accessed: Jan. 18, 2025. [Online]. Available: https://thesai.org/Downloads/Volume15No8/Paper_78-Comparative_Analysis_of_Small_and_Medium_Sized_Enterprises_Cybersecurity.pdf

[38] A. Chidukwani, S. Zander, and P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations," IEEE Access, vol. 10, pp. 85701–85719, 2022, doi: 10.1109/ACCESS.2022.3197899.

[39] I. Progoulakis, I. K. Dagkinis, A. Dimakopoulou, T. Lilas, N. Nikitakos, and P. M. Psomas, "Cyber–Physical Security Assessment for Maritime Vessels: Study on Drillship DP System Using American Petroleum Institute Security Risk Analysis and Bow-Tie Analysis," J Mar Sci Eng, vol. 12, no. 10, Oct. 2024, doi: 10.3390/jmse12101757.

[40] A. Chidukwani, S. Zander, and P. Koutsakis, "Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications," Comput Secur, vol. 145, Oct. 2024, doi: 10.1016/j.cose.2024.104026.

[41] S. R. Chourasia et al., "Cybersecurity Frameworks and Models: Review of the Existing Global Best Practices," Productivity, vol. 65, no. 1, pp. 29–42, Jun. 2024, doi: 10.32381/PROD.2024.65.01.4.

[42] V. J. Abergos and F. Medjek, "A Risk Assessment Analysis to Enhance the Security of OT WAN with SD-WAN," Journal of Cybersecurity and Privacy, vol. 4, no. 4, pp. 910–937, Dec. 2024, doi: 10.3390/jcp4040042.

[43] M. Lucchese, G. Salerno, and A. Pugliese, "A Digital Twin-Based Approach for Detecting Cyber–Physical Attacks in ICS Using Knowledge Discovery," Applied Sciences (Switzerland), vol. 14, no. 19, Oct. 2024, doi: 10.3390/app14198665.

[44] J. Domnik and A. Holland, "On Data Leakage Prevention Maturity: Adapting the C2M2 Framework," Journal of Cybersecurity and Privacy, vol. 4, no. 2, pp. 167–195, Jun. 2024, doi: 10.3390/jcp4020009.

[45] M. F. O. Santos, W. de S. Melo, A. Oliveira de Sá, M. Pasetti, and P. Ferrari, "A hybrid cyber–physical risk identification method for grid-connected photovoltaic systems," Sustainable Energy, Grids and Networks, vol. 39, Sep. 2024, doi: 10.1016/j.segan.2024.101490.

[46] S. Maesschalck, V. Giotsas, B. Green, and N. Race, "Don't get stung, cover your ICS in honey: How do honeypots fit within industrial control system security," Comput Secur, vol. 114, Mar. 2022, doi: 10.1016/j.cose.2021.102598.

[47] D. G. Rosado et al., "Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern," Comput Ind, vol. 142, Nov. 2022, doi: 10.1016/j.compind.2022.103715.

[48] O. Soner, G. Kayisoglu, P. Bolat, and K. Tam, "Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks," Applied Ocean Research, vol. 142, Jan. 2024, doi: 10.1016/j.apor.2023.103855.

[49] Marcel, Meyliana, H. L. Hendric Spits Warnars, and T. Nugraha Mursitama, "Leveraging Social Learning for Improved Cybersecurity Maturity: A Case Study Using the NIST Framework," in 2024 International Conference on Information Technology and Computing (ICITCOM), IEEE, Aug. 2024, pp. 105–110. doi: 10.1109/ICITCOM62788.2024.10762542.

[50] C. Salley, N. Mohammadi, and J. E. Taylor, "Protecting Critical Infrastructure for Disasters: NLP-Based Automated Information Retrieval to Generate Hypothetical Cyberattack Scenarios," Journal of Infrastructure Systems, vol. 30, no. 3, Sep. 2024, doi: 10.1061/JITSE4.ISENG-2407.

[51] R. Adriko and J. R. C. Nurse, "Does Cyber Insurance Promote Cyber Security Best Practice? An Analysis Based on Insurance Application Forms," Digital Threats: Research and Practice, vol. 5, no. 3, pp. 1–39, Sep. 2024, doi: 10.1145/3676283.

[52] P. Putro, D. Sensuse, and W. Wibowo, "Framework for critical information infrastructure protection in smart government: a case study in Indonesia," Information & Computer Security, vol. 32, no. 1, pp. 112–129, Jan. 2024, doi: 10.1108/ICS-03-2023-0031.

[53] O. Falowo, I. Okpala, E. Kojo, S. Azumah, and C. Li, "Exploration of Various Machine Learning Techniques for Identifying and Mitigating DDoS Attacks," in 2023 20th Annual International Conference on Privacy, Security and Trust (PST), IEEE, Aug. 2023, pp. 1–7. doi: 10.1109/PST58708.2023.10320151.

[54] R. Hopcraft, "Developing Maritime Digital Competencies," IEEE Communications Standards Magazine, vol. 5, no. 3, pp. 12–18, Sep. 2021, doi: 10.1109/MCOMSTD.101.2000073.

[55] F. Moreira, D. Da Silva Filho, G. Nze, R. T. de Sousa Junior, and R. R. Nunes, "Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology," IEEE Access, vol. 9, pp. 129605–129618, 2021, doi: 10.1109/ACCESS.2021.3113178.

[56] P. Kaliappan, S. Sudha, and D. Shankar, "International Standards for Cybersecurity in Smart Devices for the Power Sector," in 2024 International Conference on Computational Intelligence for Green and Sustainable Technologies (ICCIGST), IEEE, Jul. 2024, pp. 1–5. doi: 10.1109/ICCIGST60741.2024.10717531.

[57] R. Egan et al., "Cyber operational risk scenarios for insurance companies," British Actuarial Journal, vol. 24, p. e6, Feb. 2020, doi: 10.1017/S1357321718000284.

[58] L. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model," J Cybersecur, vol. 6, no. 1, Jan. 2020, doi: 10.1093/cybsec/tyaa005.

[59] B. Azinheira, M. Antunes, M. Maximiano, and R. P. Gomes, "Information security and cybersecurity assessment in sme-an implementation methodology," in Journal of Global Business and Technology, 2023. [Online]. Available: https://www.cncs.gov.pt/pt/roteiro-capacidades-minimas-ciberseguranaa

[60] C. Moturi, N. Abdulrahim, and D. Orwa, "Towards adequate cybersecurity risk management in SMEs," International Journal of Business Continuity and Risk Management, vol. 11, no. 4, p. 343, 2021, doi: 10.1504/IJBCRM.2021.119943.

[61] A.-M. Udroiu, M. Dumitrache, and I. Sandu, "Improving the cybersecurity of medical systems by applying the NIST framework," in 2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), IEEE, Jun. 2022, pp. 1–7. doi: 10.1109/ECAI54874.2022.9847498.

[62] R. Perdana, A. Effendy, H. Garnida, A. Fidayan, F. Nazar, and D. Saepudin, "Security and Risk Assessment of Academic Information System By Using NIST Framework (A Case Study Approach)," in 2022 16th International Conference on Telecommunication Systems, Services, and Applications (TSSA), IEEE, Oct. 2022, pp. 1–5. doi: 10.1109/TSSA56819.2022.10063890.

[63] H. Zarria Burga, B. Lecca Revilla, and D. Burga Durango, "Model to Identify the Profile of Countermeasures for Information Leakage in Financial Organizations," in 2022 IEEE Engineering International Research Conference (EIRCON), IEEE, Oct. 2022, pp. 1–4. doi: 10.1109/EIRCON56026.2022.9934810.

[64] A. Mukhopadhyay and S. Jain, "A framework for cyber-risk insurance against ransomware: A mixed-method approach," Int J Inf Manage, vol. 74, p. 102724, Feb. 2024, doi: 10.1016/j.ijinfomgt.2023.102724.

[65] J. De la Torre, D. Imbaquingo, and J. Llumiquinga, "Hybrid Information Security Framework Based on ISO/IEC 27005:2022 and the NIST Framework for the Ministry of Education of Ecuador (TIC)," 2024, pp. 71–85. doi: 10.1007/978-3-031-65285-1_6.

[66] J. Evang, "A 10-Layer Model for Service Availability Risk Management," in Proceedings of the 20th International Conference on Security and Cryptography, SCITEPRESS - Science and Technology Publications, 2023, pp. 716–723. doi: 10.5220/0012092600003555.

[67] H. Torres-Calderon, M. Velasquez, and D. Mauricio, "Method for Designing Countermeasures for Crypto-Ransomware Based on the NIST CSF," 2022, pp. 365–380. doi: 10.1007/978-981-16-3637-0_26.

[68] G. M. NIST, "Spanish Translation of the NIST Cybersecurity Framework 2.0," 2024. doi: 10.6028/NIST.CSWP.29.spa.

[69] M. L. Angelo Edú, G. P. Alexis, and W. P. Lenis, "Cybersecurity framework for SMEs in Peru based on ISO/IEC 27001 and CSF NIST controls," in 2023 18th Iberian Conference on Information Systems and Technologies (CISTI), IEEE, Jun. 2023, pp. 1–7. doi: 10.23919/CISTI58278.2023.10211874.