Implementation of the National Cyber Security Framework (NCSF) on SMEs/MSMEs Using Websites and Digital Applications: A Systematic Literature Review

Mohammad Bin Ahmed M Ali Sheikhoon
Computer Science Program, Computer Science Study Program, School of Computer Science, Bina Nusantara University, Jakarta, Indonesia 11480
Email: mohammad.sheikhoon@binus.ac.id

Abstract—**As the use of information and communication technology (ICT) continues to grow, the threat to national security posed by cyberattacks is also increasing. This study aims to evaluate the implementation of the National Cybersecurity Framework (NCF) for SMEs/MSMEs utilizing websites and digital applications. Using a systematic literature review approach, this research examines the implementation of the NCF in Indonesian SMEs/MSMEs, the key challenges encountered and its comparison with the application of similar frameworks in other countries. The findings reveal that, while the NCF encompasses critical aspects such as identification, protection, detection, response, and recovery, several weaknesses persist in its implementation. Challenges include resource constraints, a lack of cybersecurity awareness, and limited leadership support at the organizational level. The study also highlights that best practices from other countries, such as integration with CIS Controls or similar frameworks, can provide valuable insights for enhancing the NCF's implementation in Indonesia. This research is expected to contribute to strengthening national cybersecurity policies and strategies, improving SMEs/MSMEs' preparedness in addressing cyber threats, and ensuring the protection of critical data and infrastructure, which are becoming increasingly essential in the digital era.**

Keywords—Implementation of cyber security, National Cyber Security Framework, SMEs/MSMEs, Systematic Review

I. INTRODUCTION

The rapid advancement of Information and Communication Technology (ICT) has fundamentally transformed various sectors, including small and medium enterprises (SMEs) and micro, small, and medium enterprises (MSMEs). These businesses now heavily rely on digital platforms such as websites and mobile applications to enhance competitiveness, expand market reach, and optimize operations [1]. However, this growing digital dependence also exposes SMEs and MSMEs to significant cybersecurity risks, including cyberattacks that threaten their operational sustainability and customer trust [2].

Cyberattacks have become increasingly pervasive and sophisticated, targeting not only large corporations but also smaller businesses, which often lack robust cybersecurity defenses. Common threats such as phishing, malware, ransomware, and data breaches can result in financial losses, operational disruptions, and reputational damage. For SMEs/MSMEs, the consequences of such attacks are often more severe due to limited resources for recovery [3]. Studies indicate that a significant number of SMEs/MSMEs that experience cyberattacks face difficulties in recovering, with some ultimately ceasing operations altogether.

In Indonesia, the rapid growth of the digital economy has led SMEs/MSMEs to adopt digital platforms at an unprecedented rate. However, this expansion has been accompanied by an increase in cybersecurity incidents. Reports reveal that a considerable number of SMEs/MSMEs have suffered financial and data losses due to cyberattacks, highlighting the urgent need for effective cybersecurity measures [4]. Despite their growing reliance on digital technologies, many SMEs/MSMEs remain ill-prepared to address these threats, lacking both the technical expertise and financial capacity to implement comprehensive security measures.

Globally, various countries have developed cybersecurity frameworks to combat the rising threats in the digital landscape. For example: (1) United States "the National Institute of Standards and Technology (NIST) Cybersecurity Framework offers comprehensive guidelines focusing on identifying, protecting, detecting, responding to, and recovering from cyber threats. (2) United Kingdom "the Cyber Essentials framework emphasizes basic measures to protect businesses from common cyber threats. (3) India "the Data Security Council of India (DSCI) combines market-driven approaches with regulatory frameworks to address cybersecurity challenges [5].

These frameworks aim to enhance organizational resilience against cyber threats, ensuring operational continuity and the protection of critical assets. Each framework is tailored to meet the unique needs of its stakeholders, emphasizing proactive measures and collaborative efforts [6].

Received: 20-01-2025
Revised: 03-04-2025
Published: 30-06-2025

In response to the increasing incidents of cybercrime, the Indonesian government has developed the National Cybersecurity Framework (NCSF). Initially designed for government agencies, the NCSF provides structured guidance for risk assessment, asset protection, threat detection, incident response, and recovery [7]. Its scope is now being extended to SMEs/MSMEs due to their growing vulnerability to cyber threats. The NCSF emphasizes the following key components: (1) Risk assessment "identifying potential vulnerabilities and threats". (2) Protective measures "implementing safeguards to secure digital assets. (3) Detection mechanisms "monitoring systems for early identification of threats. (4) Response strategies "establishing protocols for effective incident management". (5) Recovery plans "ensuring business continuity after an attack [8].

Existing studies on cybersecurity frameworks highlight their critical role in enhancing digital resilience. Research comparing frameworks like NIST, ISO/IEC 27001, and others underscores the importance of context-specific adaptations for effective implementation [9]. For SMEs/MSMEs, studies reveal that adopting frameworks tailored to their resource constraints and operational needs significantly improves their cybersecurity posture.

In Indonesia, initial applications of the NCSF in government agencies have demonstrated its potential to mitigate risks and enhance system integrity. However, research on its application in the SME/MSME sector remains limited [10]. This study seeks to fill this gap by evaluating the NCSF's effectiveness in SMEs/MSMEs, identifying challenges in its adoption and providing actionable recommendations to optimize its implementation.

This research critically examines the application of the NCSF within Indonesian SMEs/MSMEs that utilize digital platforms. It aims to evaluate the extent of NCSF implementation in these sectors, identify challenges faced during its adoption, analyze factors influencing its effectiveness dan compare NCSF implementation with international best practices [11].

The findings are expected to offer practical insights for policymakers and business owners, supporting the development of robust cybersecurity strategies that align with global standards while addressing local needs. By strengthening cybersecurity in SMEs/MSMEs, this research contributes to fostering a secure and resilient digital economy in Indonesia.

II. Review Methodology

Cybersecurity has become one of the main concerns in the digital era, particularly for small and medium-sized enterprises (SMEs) and micro, small, and medium-sized enterprises (MSMEs) that are increasingly dependent on information and communication technology. In this context, the National Cyber Security Framework (NCSF) is designed to assist government agencies in assessing and improving the security of their information technology infrastructure [9].

The NCSF framework encompasses a structured approach consisting of standards, procedures, and policies designed to protect systems and data from increasingly complex cyber threats. The NCSF is based on five core elements: Identify to recognize assets, risks, and vulnerabilities, protect to develop measures to secure the system, detect to identify incidents and suspicious activities early, respond to manage and mitigate security incidents and recover to restore operational conditions after an incident occurs [12].

These elements are interconnected to ensure comprehensive cybersecurity. In this study, the NCSF is adapted to evaluate its implementation in the SMEs/MSMEs sector, which relies on digital platforms such as websites and applications. The focus of this adaptation is to provide practical insights for strengthening cybersecurity for businesses that typically have limited IT resources and technical expertise [13].

In addition to the NCSF, this study also utilizes the Critical Security Controls (CIS Controls) framework developed by the Center for Internet Security (CIS). CIS Controls is a set of core controls that includes 18 categories with 153 sub-controls to strengthen an organization's cybersecurity. These controls are not intended to replace existing frameworks but to complement them with practical steps designed to simplify the complex cybersecurity requirements and enhance overall cybersecurity defense. Key categories of CIS Controls include: (1) asset and data management, (2) hardware and software security, (3) threat detection and response, and (4) network monitoring and user access.

This study employs the Systematic Literature Review (SLR) method to explore the application of the NCSF and similar frameworks in the SMEs/MSMEs sector. This approach is carried out through the following stages [14]: (1) Data Collection "Identifying and gathering relevant literature from journals, research reports, and best practice guidelines related to cybersecurity." (2) Framework Mapping "Analyzing the elements of NCSF and CIS Controls to build a deep understanding of the functionality of each element." (3) Identification of Current Conditions and Objectives "Assessing the readiness of SMEs/MSMEs in implementing cybersecurity frameworks." (4) Gap Analysis "Identifying the differences between current practices and the ideal proposed cybersecurity standards." (5) Recommendations and Action Plan"Providing evidence-based recommendations to improve cybersecurity for SMEs/MSMEs."

For comparison, this study also examines several cybersecurity frameworks adopted in other countries, including [5]: (1) NIST Cybersecurity Framework (US) "A comprehensive cybersecurity guide developed by the National Institute of Standards and Technology." This framework includes a risk-based approach to identify, protect, detect, respond to, and recover from cyber incidents. (2) UK Cyber Essentials (UK) "A cybersecurity certification scheme aimed at protecting businesses from common threats." This scheme focuses on basic measures such as firewalls, access control, and software patching. (3) ISO/IEC 27001 (Global) "An international standard for Information Security Management Systems (ISMS), offering a process-based approach to protecting sensitive information."

This study gives special attention to the adaptation of the NCSF and CIS Controls elements in the context of SMEs/MSMEs in Indonesia, considering their resource limitations. Furthermore, the comparative analysis with international frameworks provides additional insights to understand the potential for developing better cybersecurity strategies.

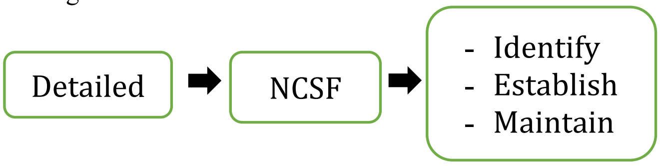

Fig.1 Applied Framework

The mapping of the National Cyber Security Framework (NCS) in the context of SMEs (Small and Medium Enterprises) and MSMEs (Micro, Small and Medium Enterprises) can be seen in Fig. 1. For example, the concept of "Establish and Maintain Detailed Asset Inventory" in the NCS is aligned with the Identification security function, which is critical for businesses to recognize critical assets, including digital platforms such as websites and applications. This concept is expanded and adapted to meet the specific needs of SMEs/MSMEs, which often face resource constraints in managing assets compared to larger organizations.

The first stage involves building an understanding of the current cybersecurity conditions of SMEs/MSMEs. This study adopts the tiered approach of the NCSF framework, which categorizes organizational readiness into four levels: (1) Level 1: Partial, (2) Level 2: Risk-Aware, (3) Level 3: Repeatable and (4) Level 4: Adaptive.

With a focus on the human resource capabilities and technical infrastructure of SMEs, the framework is tailored to their specific context.

The next stage involves a gap analysis to identify differences between current cybersecurity practices and desired targets. The study aims to achieve an average target condition score equivalent to Level 3: Repeatable, indicating consistent and systematic implementation of cybersecurity practices. Achieving this target requires collaboration with stakeholders to improve cybersecurity strategies, including the implementation of best practices and decision-making related to application development.

Following the gap analysis, recommendations are formulated to address these gaps. For SMEs, the recommendations focus on cost-effective solutions such as: (1) Leveraging open-source cybersecurity tools, (2) Conducting regular cybersecurity awareness training. (3) Implementing basic but critical measures, such as data backup and endpoint protection.

Finally, a Proposed Action Plan is developed to address high, medium, and low priority issues. The plan includes actionable steps tailored to SMEs, emphasizing minimizing the risk of cyberattacks while enhancing cybersecurity in their digital infrastructure.

The study systematically analyzes selected cybersecurity frameworks, including their adaptation and implementation in SMEs. By comparing the NCSF with other frameworks, the study identifies best practices and assesses their suitability for enhancing cybersecurity in SMEs. The analysis provides insights and actionable recommendations to improve the implementation of the NCSF in the SME context, ensuring that these businesses can safely leverage digital technologies to sustain growth and competitiveness.

Table 1
Comparison Of Various Cybersecurity Development Frameworks Based On Relevant Content

Criteria	Implementation Status in NCSF for SMEs/MSMEs	Information
Strategy Development		
Supported by Strong Leadership	X	Leadership support exists but needs adaptation to SME/MSME needs.
Multi-Stakeholder Approach	X	Collaboration with stakeholders, including SME/MSME owners and developers.
Clear Cybersecurity Vocabulary Definition	X	Standardized cybersecurity definitions are established.
Inform and Educate Key Players	X	Awareness programs targeting SMEs/MSMEs.
Strategy Delivery		
Sustainable Progress Reporting	X	Reports on cybersecurity adoption among SMEs/MSMEs.
Supervision by Special Institutions	X	Oversight from designated cybersecurity bodies.
Strategy Overview		

Criteria	Implementation Status in NCSF for SMEs/MSMEs	Information
Sustainable Monitoring and Validation	X	Continuous process for ensuring effectiveness in SME/MSME settings.
Periodic Review	X	Regular reviews to align with SME/MSME growth.
Introduction and Background Section		
Current Status of National Cybersecurity	X	Assessment of SME/MSME cybersecurity maturity.
Cybersecurity Challenges Presentation	X	Identification of challenges specific to SMEs/MSMEs.
Justification for Strategy Development	X	Clear rationale for targeting SMEs/MSMEs in the cybersecurity framework.
Guiding Principles		
Strategy Based on National Values	X	Aligns with Indonesia's national cybersecurity values.
Respect Privacy and Protect Civil Liberties	X	Privacy protection integrated into SME/MSME-focused strategies.
Risk-Based Approach	X	Risk assessments tailored to SMEs/MSMEs.
Vision and Strategy		
Promoting Economic Development	X	Supportive of SME/MSME growth through secure digital adoption.
Providing National Leadership	X	Effective leadership facilitating SME/MSME inclusion.
Addressing Cybercrime	X	Cybercrime prevention measures targeting vulnerabilities in SMEs/MSMEs.
Strengthening Critical Infrastructure	X	Enhanced security for digital platforms used by SMEs/MSMEs.
Raising Awareness	X	Public awareness campaigns focusing on SME/MSME cybersecurity.
Fostering Shared Responsibility	X	Collaboration among SMEs/MSMEs, government, and stakeholders.
Building National and International Partnerships	X	Partnerships to strengthen SME/MSME cybersecurity capabilities.
Risk Management		

Criteria	Implementation Status in NCSF for SMEs/MSMEs	Information
Explain Risk Management Methods	X	Tailored methods for SMEs/MSMEs.
Identify Threats and Vulnerabilities	X	Vulnerability assessments for digital SME/MSME operations.
Categorize Risks	X	Risks classified for actionable prioritization.
Avoid Creation of National Standards to Prevent ICT Supply Chain Deviations	X	Standards maintained for consistency in SME/MSME digital environments.
SMART Goals	X	Goals aligned with specific SME/MSME security outcomes.
Strategy Implementation		
Governance and Management Structure	X	Governance frameworks adapted for SME/MSME contexts.
Legal and Regulatory Framework	X	Compliance with existing laws applied to SMEs/MSMEs.
Capacity Building	X	Training programs enhancing SME/MSME cybersecurity skills.
Awareness	X	Ongoing education initiatives.
Incident Countermeasures	X	Response protocols adapted to SME/MSME scale.
Stakeholder Collaboration	X	Coordination among SMEs/MSMEs and cybersecurity agencies.
Research and Development	X	Focus on SME/MSME-specific cybersecurity solutions.
Monitoring and Evaluation	X	Sustainable monitoring practices implemented.

Based on Table 1, the implementation status of the National Cyber Security Framework (NCSF) specifically designed for SMEs/MSMEs utilizing digital websites and applications. "X" indicates that specific criteria have been implemented in accordance with the NCSF guidelines. The adaptation focuses on meeting the unique needs of SMEs/MSMEs, ensuring that cybersecurity strategies are cost-effective and scalable. This systematic comparison underscores the relevance and applicability of the NCSF to enhance cybersecurity resilience among SMEs/MSMEs in Indonesia.

III. Results and Discussion

There are many cases of cyber attacks that occur in Indonesia and are rampant, one of which is in the sector we are discussing, namely MSMEs/UKMs, attacks ranging from fraud (scams), which are targeted on average because of reputation issues/dirty competition in their product market.

From several sources around 55% of MSMEs/UKMs experience cyber attacks, because now they have switched to using digitalization, such as using marketplaces to sell, such as phishing, SQL injection, etc., there are many cases of MSMEs experiencing cyber attacks that harm their businesses and also the country because MSMEs/UKMs are the mainstay of the Indonesian economy which contributes 60.5% of Indonesia's GDP (Gross Domestic Product).

The current security posture assessment aims to provide a comprehensive understanding of the security status of websites and digital applications used by SMEs/MSMEs. The process focuses on critical elements such as functionality, performance, security, and usability, with a special emphasis on cybersecurity. The evaluation is conducted as part of a systematic initiative to improve application resilience, address vulnerabilities, and enhance user trust [15].

Security assessments for websites and applications can be performed using methods such as direct observation, questionnaires, or document analysis. A common tool for evaluating the severity of identified vulnerabilities is the Common Vulnerability Scoring System (CVSS). CVSS assigns a numerical score that categorizes severity into three levels: (1) Low: Scores from 0.0 to 3.9, (2) Medium: Scores from 4.0 to 6.9. (3) High: Scores from 7.0 to 10.0 [16].

This scoring system provides SME/SME owners and managers with an understanding of cybersecurity risks and informs decisions about necessary mitigation measures. In this study, the most frequently identified vulnerability was SQL Injection, which received a high severity rating. This vulnerability leaves digital applications vulnerable to unauthorized access and potential data breaches. To address this, the researchers proposed a mitigation strategy aligned with the National Cyber Security Framework (NCSF). The strategy involves reviewing and remediating the application source code to eliminate SQL Injection vulnerabilities [17].

This approach underscores the importance of following the NCSF principles of comprehensive protection for information systems and applications. By implementing these strategies, SMEs can strengthen their cybersecurity posture, ensure more secure applications, and significantly reduce the risk of cyberattacks. The systematic literature review also revealed that SMEs often face challenges in maintaining strong cybersecurity practices due to limited resources and technical expertise. Therefore, implementing a framework such as the NCSF is critical to provide a structured and scalable roadmap tailored to the unique needs of these organizations.

This systematic review states that it is important to adopt a standard framework to encourage better cybersecurity practices among SMEs/MSMEs while ensuring alignment with national cybersecurity objectives.

Table 2
List of Vulnerabilities from Assessment Results and Mitigation Actions

Vulnerability Name	Severity Level Before Mitigation	Severity Level After Mitigation
SQL Injection	High	Not found
Application Error Messages	Medium	Medium
Directory Listings	Medium	Medium

Table 2 presents the results of vulnerability assessments conducted on websites and digital applications used by SMEs/MSMEs, both before and after the implementation of mitigation measures. The results show that SQL Injection, which poses a critical threat with a high severity, was successfully eliminated after the implementation of mitigation strategies involving application source code fixes. Other vulnerabilities, such as Application Error Message and Directory Listing, remained at a Medium severity level even after the mitigation measures. These findings suggest that while the implemented strategies are effective in addressing critical vulnerabilities such as SQL Injection, additional measures may be needed to further reduce the severity of less critical vulnerabilities [17].

This assessment demonstrates the alignment of mitigation efforts with the principles of the National Cybersecurity Framework (NCSF), which emphasizes prioritizing critical vulnerabilities to improve the security and resilience of information systems and applications.

Implementing targeted and measurable mitigation actions is critical to addressing high-priority threats while continuing to improve the overall cybersecurity posture. Moderate vulnerability resilience highlights the need for ongoing monitoring, refinement of security practices, and possible implementation of more sophisticated mitigation techniques.

After collecting and analyzing the data, as shown in Table 3, the CIS Controls framework was mapped to the National Cybersecurity Framework (NCSF) as applied to SMBs using digital websites and applications. This mapping demonstrates how the CIS Controls can complement the NIST Cybersecurity Framework, with a focus on more granular implementations.

Table 3
Mapping of Cybersecurity Frameworks

Security Functions	Number of Concepts in the Applied Framework
NIST Cybersecurity Framework	
Identify	23
Protect	28
Detect	16
Respond	12
Recover	5
Total	84

From Table 3, it can be seen that the security function "Identify" covers 23 concepts from the NIST Cybersecurity Framework. Meanwhile, other functions such as Protect, Detect, Respond, and Recover provide a total of 84 concepts.

This mapping shows how the NCSF applied to SMEs/MSMEs still focuses on the NIST framework without the addition of concepts from CIS Controls. This underscores the need to consider further integration of relevant concepts to address the specific cybersecurity challenges faced by SMEs/MSMEs in a digital context.

After the framework mapping process is complete, the next stage is to identify the current security conditions. This process aims to assess the level of security in the system or application being evaluated, covering various aspects such as data, network, and application security. In addition, identification also includes the implementation of existing security features. [18].

Hasil identifikasi dirangkum dalam Tabel 4, yang The identification results are summarized in Table 4, which shows the average current security condition score of 2.61, in accordance with Tier 2 - Risk Informed in the NCSF framework. Furthermore, discussions were conducted with application managers to determine the desired or desired conditions. Based on the agreement, the desired condition for each security function was targeted with an average score of 3.00, in accordance with Tier 3 - Repeatable in the NCSF framework.

Table 4
Identification of Current Conditions and Desired/Achieved Conditions

Security Functions	Present condiition	Desired/Achieved Condition
Identification	2,67	3,00
Protection	2,73	3,00
Detection	2,79	3,00
Response	2,65	3,00
Recovery	2,21	3,00
Average	2,61	3,00

From Table 4, it can be explained that one of the security functions, namely Identification, shows a current condition with an average score of 2.67, while the desired condition is 3.00. Similar things can be seen in other functions, where all desired conditions have an average target value of 3.00. This table also shows that the Recovery function has the lowest current condition score, namely 2.21, indicating the need for greater focus on improvement in this area. Upgrading all security functions to Tier 3 - Repeatable will help ensure that cybersecurity measures in SMEs/MSMEs that use websites and digital applications can be carried out consistently and effectively.

Based on the results of the gap analysis conducted, it was found that there is a difference between the current cybersecurity conditions and the desired or achieved conditions in the implementation of the National Cyber Security Framework (NCSF) in SMEs/MSMEs that use websites and digital applications. The average gap identified was 0.23, indicating that there is still room for improvement in several aspects of cybersecurity.

Table 5
Summary of Gap Analysis

Security Functions	Present condiition	Desired/Achieved Condition	The Gap
Identification	2,79	3,00	0,21
Protection	2,82	3,00	0,18
Detection	2,88	3,00	0,12
Response	2,80	3,00	0,20
Recovery	2,53	3,00	0,47
Average	2,77	3,00	0,23

Based on Table 5 on the security function "Protection," researchers highlighted the lack of cybersecurity training for all system users, as well as the lack of implementation of procedures and processes that support monitoring and risk management in accordance with information security standards.

In the "Detection" function, there were deficiencies in the monitoring procedures for cyber threats such as malicious code and mobile software. This indicates that there is still a need to develop more effective procedures to detect potential threats. In the "Response" function, the procedures implemented to respond to cybersecurity incidents also do not fully cover all necessary aspects, indicating the need for further improvement.

On the other hand, in the "Recovery" function, the biggest gap was found in the absence of documented policies and procedures for handling and recovering from incidents. Although there have been no significant cyber incidents, creating preventive measures and documenting incident handling is essential to ensure preparedness if an incident occurs in the future.

Recommendations to reduce the existing gaps include strengthening cybersecurity policies and procedures, improving user training, and developing more comprehensive documentation on incident handling and recovery. These recommendations must be implemented after obtaining approval from the structural leadership at the relevant agency.

The results of the study showed that support from top leaders in many SMEs/MSMEs that use websites and digital applications is still limited, which hinders the implementation of cybersecurity policies even though some policies have been implemented. Strong leadership and involvement of various stakeholders, including the private sector, academia, and the community, are essential to improve the effectiveness of this policy. Definitions and explanations of cybersecurity terms in the policy are also often inadequate, causing confusion among implementers [19].

In addition, education and training strategies need to be strengthened to improve preparedness for evolving cyber threats. Annual reports on the implementation of cybersecurity strategies are often inaccurate, while oversight by cybersecurity-focused agencies in Indonesia still needs to be improved. Continuous monitoring of the policy and the absence of periodic reviews also cause the policy to become outdated.

The governance structure for implementing cybersecurity policies is often unclear, hampering effective implementation [20]. Capacity building in the justice and law enforcement sectors is also lacking, and non-standardized risk management methods lead to misalignment in risk management. Collaboration with internet service providers (ISPs) and international entities on cyber protection in Indonesia still needs to be strengthened.

Key challenges in policy implementation include lack of leadership support, limited training, and ineffective governance structures. To improve the implementation of the National Cyber Security Framework (NCSF) in the future, there is a need for increased leadership support, development of more comprehensive training, and establishment of a clearer governance structure. Collaboration and partnerships at the national and international levels must also be strengthened to improve cyber defense as a whole.

When assessing the cybersecurity posture of SMEs, it is important to consider the scale and complexity of the digital applications used. SMEs typically use websites and applications with limited functions that focus on specific services or products. This simplicity provides the advantage of reducing potential attack surfaces. However, on the other hand, vulnerabilities such as SQL Injection, as previously mentioned, can have significant impacts on their operations.

A. Comparison of NCSF with Other Frameworks

When comparing the National Cyber Security Framework (NCSF) with other cybersecurity frameworks, there are several key differences. First, the NIST Cybersecurity Framework (NIST CSF), developed by the National Institute of Standards and Technology, offers a risk based approach to managing cybersecurity threats [21]. Comprising five core functions Identify, Protect, Detect, Respond, and Recover NIST CSF is highly flexible and widely adopted, including by SMEs. Second, ISO/IEC 27001, with its international standard, focuses on Information Security Management Systems (ISMS). Its systematic approach ensures the confidentiality, integrity, and availability of information. However, the ISO 27001 certification process can be costly and resource-intensive, which is often a challenge for SMEs. Third, CIS Controls, developed by the Center for Internet Security, provides a set of prioritized, practical steps to protect against common cyber threats [22]. These steps are highly useful for SMEs with limited resources. NCSF aligns with other frameworks in promoting a structured approach to cybersecurity, but its advantage lies in its flexibility and focus on scalability, making it particularly well-suited for SMEs.

B. Relationship Between NCSF Framework and SME Applications

The implementation of NCSF in the context of SME applications involves several key considerations. First, Resource Allocation: With limited resources, the gradual approach of NCSF allows SMEs to progressively enhance their cybersecurity posture without overburdening their capacity [23]. Second, Security Control Adaptation: NCSF encourages the customization of security controls to align with the specific needs and risk profiles of SMEs, ensuring that the implemented measures are both effective and efficient [24]. Third, Integration with Business Processes: By aligning cybersecurity efforts with business objectives, NCSF helps SMEs seamlessly integrate security into their daily operations, fostering a culture of security awareness and resilience [25].

Although various cybersecurity frameworks provide valuable guidelines, the flexibility and focus on scalability offered by NCSF make it highly beneficial for SMEs. By adopting NCSF, SMEs can develop robust cybersecurity practices tailored to their operational context, thereby enhancing resilience against cyber threats.

IV. CONCLUSION

The implementation of the National Cyber Security Framework (NCSF) on SMEs/MSMEs that use digital websites and applications shows significant effectiveness and opportunities. Based on the analysis and evaluation, the main conclusions are as follows: First, support from top leaders in many government agencies is still limited, which affects the effectiveness of cybersecurity policies. To improve the implementation of the NCSF, strong leadership is needed from the private sector, academia, and the general public. This includes efforts to raise awareness of cybersecurity and the development of more comprehensive training programs. Second, the application security assessment shows that some vulnerabilities, such as SQL Injection, have been successfully addressed through appropriate mitigation steps. However, other vulnerabilities, such as Application Error Messages and Directory Listings, still require further attention. Appropriate mitigation based on the NCSF principles can significantly reduce risks and improve the digital security of SMEs/MSMEs. Third, the framework mapping shows that the CIS Controls provide additional details that complement the NIST Cyber Security Framework (NCSF). The integration of these two frameworks is considered important to provide a more holistic cybersecurity approach tailored to the needs of SMEs/MSMEs. Fourth, the gap analysis identified an average gap of 0.23 between the current and desired security conditions. The largest gap was found in the Recovery function, highlighting the need for clearer and more structured incident handling documentation policies and procedures. It also underlines the need to strengthen the steps in the Identify, Protect, Detect, and Respond functions. Fifth, to address this gap, SMEs are recommended to strengthen cybersecurity policies and procedures, conduct regular user training, develop comprehensive incident handling documentation, increase leadership support, clarify cybersecurity governance structures, and strengthen collaboration and partnerships both nationally and internationally. Moreover, MSMEs are distributors of Indonesia's GDP (Gross Domestic Product), therefore the government must protect and pay attention to matters related to cyber attacks.

REFERENCES

[1] N. Samsudin, J. Osman, N. A. Jalil, and T. Zakaria, “A Recent Systematic Review on Digital Marketing Transformation and Business Performance,” *J. Adv. Res. Appl. Sci. Eng. Technol. 59*, vol. 1, no. 1, pp. 52–67, 1943.

[2] A. Papathanasiou, G. Liontos, A. Katsouras, and V. Liagkou, “Cybersecurity Guide for SMEs : Protecting Small and Medium-Sized Enterprises in the Digital Era,” *J. Inf. Secur.*, vol. 16, no. 1, pp. 1–43, 2025, doi: 10.4236/jis.2025.161001.

[3] J. R. Batmetan, “A Cyber Security and Digital Transactions to Educated the Micro, Small and Medium Business Community,” *Int. J. Inf. Technol. Educ.*, vol. 2, no. 4, pp. 1–11, 2023, doi: 10.62711/ijite.v2i4.152.

[4] Shama, S. S. Mazhar, A. U. Rehman, and F. S. Khan, “How digital technology and innovation can be leveraged in small and medium enterprises: a bibliometric analysis,” *Int. J. Technol. Learn. Innov. Dev.*, vol. 15, no. 2, pp. 162–182, 2023, doi: 10.1504/IJTLID.2023.135341.

[5] A. Mishra, Y. I. Alzoubi, M. J. Anwar, and A. Q. Gill, “Attributes impacting cybersecurity policy development: An evidence from seven nations,” *Comput. Secur.*, vol. 120, 2022, doi: 10.1016/j.cose.2022.102820.

[6] Y. Khan *et al.*, “Public health emergency preparedness: a framework to promote resilience,” *BMC Public Health*, vol. 18, no. 1, pp. 1–16, 2018, [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6280369/pdf/12889_2018_Article_6250.pdf

[7] N. D. Nte, B. K. Enoke, and A. Teru, "A Comparative Analysis of Cyber Security Laws and Policies in Nigeria and South Africa OPEN ACCESS," *LAW Res. Rev. Q.*, vol. 8, no. 2, pp. 233–258, 2022.

[8] R. J. Cramer *et al.*, "Preferences in information processing, marginalized identity, and non-monogamy: Understanding factors in suicide-related behavior among members of the alternative sexuality community," *Int. J. Environ. Res. Public Health*, vol. 17, no. 9, pp. 1–17, 2020, doi: 10.3390/ijerph17093233.

[9] L. Liyanage, N. A. G. Arachchilage, and G. Russello, "SoK: Identifying Limitations and Bridging Gaps of Cybersecurity Capability Maturity Models (CCMMs)," pp. 1–35, 2024, [Online]. Available: http://arxiv.org/abs/2408.16140

[10] R. Is, S. Kv, and S. Hungund, "MSME / SME Financial Literacy : A Systematic Literature Review and Bibliometric Analysis," *J. Knowl. Econ.*, no. 0123456789, 2024, doi: 10.1007/s13132-024-02472-0.

[11] Tina Vuko, *Key drivers of cybersecurity audit effectiveness: A neo-institutional perspective*. 2023, pp. 1–19.

[12] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," *Eurasip J. Inf. Secur.*, vol. 2020, no. 1, 2020, doi: 10.1186/s13635-020-00111-0.

[13] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," *Sensors*, vol. 23, no. 15, pp. 1–20, 2023, doi: 10.3390/s23156666.

[14] M. E. Fernandez *et al.*, "Implementation mapping: Using intervention mapping to develop implementation strategies," *Front. Public Heal.*, vol. 7, no. JUN, pp. 1–15, 2019, doi: 10.3389/fpubh.2019.00158.

[15] A. AL-Hawamleh, "Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security," *Int. J. Comput. Digit. Syst.*, vol. 15, no. 1, pp. 1315–1331, 2024, doi: 10.12785/ijcds/150193.

[16] N. A. Azeez and C. Van der Vyver, "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis," *Egypt. Informatics J.*, vol. 20, no. 2, pp. 97–108, 2019, doi: 10.1016/j.eij.2018.12.001.

[17] A. Paul, V. Sharma, and O. Olukoya, "SQL injection attack: Detection, prioritization & prevention," *J. Inf. Secur. Appl.*, vol. 85, no. August, p. 103871, 2024, doi: 10.1016/j.jisa.2024.103871.

[18] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the IoT: A Survey of Existing Protocols and Ope Research issues," *IEEE Commun. Surv. Tutorials*, pp. 1–20, 2013.

[19] A. Althonayan and A. Andronache, "Shifting from information security towards a cybersecurity paradigm," *ACM Int. Conf. Proceeding Ser.*, no. September 2018, pp. 68–79, 2018, doi: 10.1145/3285957.3285971.

[20] W. Aman and J. Al Shukaili, "A Classification Of Essential Factors For The Development And Implementation Of Cyber Securitym Strategy In Public Sector Organizations," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 8, pp. 169–176, 2021, doi: 10.14569/IJACSA.2021.0120820.

[21] M. Alshar'e, "Cyber Security Framework Selection: Comparision of Nist and Iso27001," *Appl. Comput. J.*, vol. 3, no. 1, pp. 245–255, 2023, doi: 10.52098/acj.202364.

[22] R. Rohan, B. Papasratorn, W. Chutimaskul, J. Hautamäki, S. Funilkul, and D. Pal, "Enhancing Cybersecurity Resilience: A Comprehensive Analysis of Human Factors and Security Practices Aligned with the NIST Cybersecurity Framework," *ACM Int. Conf. Proceeding Ser.*, no. December, 2023, doi: 10.1145/3628454.3629472.

[23] E. M. Raineri, L. S. E. Reno, B. Krapf, and T. Croy, "Marketing Ethics: A Study of Significance Within National Professional Associations," *J. Leadership, Account. Ethics*, vol. 20, no. 2, pp. 46–65, 2023, doi: 10.33423/jlae.v20i2.6257.

[24] S. Pete, C. Katherine, N. Johnson, C. Donovan, and C. Francesco, "Global Change Biology - 2019 - Smith - Which practices co-deliver food security climate change mitigation and adaptation .pdf." 2019.

[25] W. Viriyasitavat, L. Da Xu, Z. Bi, and A. Sapsomboon, "Blockchain-based business process management (BPM) framework for service composition in industry 4.0," *J. Intell. Manuf.*, vol. 31, no. 7, pp. 1737–1748, 2020, doi: 10.1007/s10845-018-1422-y.