JIRBDAI

Journal of Institutional Research, Big Data Analytics and Innovation

Cybersecurity Maturity Model for Small and Medium-Sized Enterprises

Denis Tersoo Michael, Abdullahi Musa Yola
Computer Science Department, Faculty of Science, Federal University of Kashere, Gombe State, Nigeria.
michaeltes24@gmail.com, amyola@fukashere.edu.ng

ABSTRACT

Small and Medium Enterprises (SMEs) increasingly rely on digital technologies to support their business operations, yet they remain highly vulnerable to cyber threats due to limited cybersecurity resources and expertise. Existing cybersecurity maturity models are often designed for large organizations and may not adequately address the operational realities of SMEs. This study proposes a context-aware cybersecurity maturity framework tailored to the needs of SMEs and validates it through a rigorous three-stage process involving expert panel evaluation, content validity assessment, and empirical pilot testing. The framework is structured around five key cybersecurity domains: governance, human resource security, asset management, access control, and threat management. A five-level maturity scale was adopted to assess cybersecurity practices across these domains. The proposed framework was applied to 42 SMEs across six industry sectors to determine the maturity level of cybersecurity practices and identify areas requiring improvement. The results show varying maturity levels across domains, with access control demonstrating the highest maturity level ($M = 3.89$, $SD = 0.52$), while threat management ($M = 2.18$, $SD = 0.76$) and asset management ($M = 2.34$, $SD = 0.81$) recorded the lowest maturity levels. Statistical analysis revealed significant differences across domains ($F(4, 205) = 47.32$, $p < 0.001$), with threat management significantly lagging behind all other domains. The Cronbach's alpha for the overall assessment instrument was 0.87, indicating good internal consistency. A comparative analysis with established frameworks (NIST CSF 2.0, C2M2, CIS Controls v8, and ISO/IEC 27001) demonstrates that the proposed model offers unique advantages in terms of SME scalability, resource efficiency, and progressive implementation guidance. The proposed model provides a scalable and practical approach that supports SMEs in identifying gaps and improving cybersecurity readiness.

KEYWORDS: Cybersecurity Maturity Model; Small and Medium Enterprises; Cyber Resilience; Asset Management; Threat Management; Access Control.

I. INTRODUCTION

The increasing digitalization of business processes has significantly expanded the cybersecurity threat landscape for organizations across the world. Modern enterprises rely heavily on interconnected information systems, cloud computing services, and online communication platforms to support their operations. While these technologies enhance efficiency and productivity, they also introduce significant cybersecurity vulnerabilities that can be exploited by cybercriminals (European Union Agency for Cybersecurity, 2024). Recent studies indicate that cyberattacks such as ransomware, phishing, and data breaches continue to increase globally, causing severe financial and reputational damage to organizations (Alshboul, Ghani, & Alqudah, 2021). Small and Medium Enterprises (SMEs) represent a critical component of most national

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.21599002

economies, yet they remain among the most vulnerable organizations to cyber threats. SMEs often operate with limited financial resources, inadequate cybersecurity expertise, and insufficient security infrastructure, making them attractive targets for cyber attackers. Research by Coventry and Branley (2021) shows that many SMEs lack formal cybersecurity strategies and structured risk management practices, which significantly increases their exposure to cyber risks. Similarly, Bada, Sasse, and Nurse (2021) revealed that low cybersecurity awareness among SME employees and management contributes to weak implementation of security policies and controls.

To address these cybersecurity challenges, several organizations have developed security frameworks and standards to guide the implementation of cybersecurity practices. These frameworks provide guidelines for identifying risks, protecting digital assets, detecting cyber incidents, and responding to security breaches. However, Poeppelbuss, Niehaves, and Simons (2021) argue that comprehensive cybersecurity frameworks are often complex and resource-intensive, which makes them difficult for SMEs to adopt effectively. Many SMEs lack the technical expertise and financial capacity required to fully implement such comprehensive security standards. Cybersecurity maturity models have therefore emerged as practical tools that allow organizations to assess their current cybersecurity capabilities and identify areas for improvement. Maturity models provide structured mechanisms for evaluating cybersecurity practices across different organizational domains and classifying them into progressive levels of development. Despite the growing adoption of cybersecurity maturity models, many existing frameworks are primarily designed for large organizations and may not adequately reflect the operational realities and resource constraints faced by SMEs. Studies by Coventry & Branley (2023) emphasize the need for simplified and scalable cybersecurity maturity frameworks tailored specifically to SMEs. Such frameworks should focus on critical security domains while providing practical guidance that enables SMEs to progressively enhance their cybersecurity capabilities. Therefore, this study aims to design and validate a context-aware cybersecurity maturity framework that supports SMEs in assessing their cybersecurity posture and systematically improving their security practices. The specific objectives of this study are: (1) to design a context-aware cybersecurity maturity framework tailored to the resource constraints and operational realities of SMEs; (2) to validate the proposed framework through expert evaluation and empirical testing; (3) to assess the current cybersecurity maturity level of SMEs across the five key domains.

II. RELATED WORKS

A. Cybersecurity Challenges Facing SMEs

Small and Medium Enterprises (SMEs) is important in economic development, innovation, and employment generation across many countries. They represent a large proportion of businesses globally and contribute significantly to national productivity and economic stability. Despite their importance, SMEs face considerable cybersecurity challenges that expose them to various forms of cyber threats. With the rapid adoption of digital technologies such as cloud computing, online payment systems, e-commerce platforms, and remote work infrastructures, SMEs have increasingly become targets for cybercriminals. This growing reliance on digital technologies has expanded the attack surface of SMEs and made them vulnerable to cyber threats such as phishing attacks, ransomware, malware, and data breaches (Heidt, Gerlach, & Buxmann, 2019). One of the most significant cybersecurity challenges faced by SMEs is the limited availability of financial and technical resources required to implement effective cybersecurity measures. Unlike

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.21599002

large organizations that can allocate substantial budgets to cybersecurity infrastructure, SMEs often operate under tight financial constraints and prioritize investments that directly support business operations and growth. Consequently, cybersecurity investments are frequently overlooked or underfunded. Research by Puhakainen and Siponen (2010) indicates that organizations with limited financial resources often struggle to adopt advanced cybersecurity technologies and protective systems. Similarly, Heidt, Gerlach, and Buxmann (2019) observed that SMEs typically lack dedicated IT security professionals and advanced technological infrastructure, which limits their ability to detect, prevent, and respond to cyber incidents effectively.

Another challenge faced by SMEs is the misconception that cybercriminals primarily target large corporations rather than small businesses. This perception often results in a false sense of security among SME owners and managers, leading them to underestimate the importance of investing in cybersecurity measures. However, research suggests that cyber attackers frequently target SMEs because they tend to have weaker security defenses and limited detection capabilities. Hadlington (2017) notes that the lack of cybersecurity awareness and preparedness among SMEs makes them attractive targets for cybercriminals seeking easy entry points into digital systems. SMEs face growing cybersecurity risks associated with their participation in interconnected supply chains and digital business ecosystems. As SMEs increasingly collaborate with larger organizations, vendors, and partners through shared digital platforms and information systems, vulnerabilities within SME networks can expose entire supply chains to cyber threats. According to Ahmad, Bosua, and Scheepers (2014), cyber attackers may exploit weaknesses in smaller organizations to gain unauthorized access to larger corporate networks within supply chains. This situation highlights the importance of strengthening cybersecurity capabilities within SMEs not only for their own protection but also for the security of broader business networks.

B. Cybersecurity Maturity Models

Cybersecurity maturity models have emerged as structured tools that help organizations evaluate the effectiveness of their cybersecurity capabilities and identify areas requiring improvement. These models provide systematic frameworks for assessing security practices across different organizational domains and classifying them into progressive levels of maturity. By adopting maturity-based assessments, organizations can determine their current cybersecurity posture and develop strategic plans for improving their resilience against cyber threats. According to Poeppelbuss, Niehaves, Simons, and Becker (2021), maturity models are widely used in information systems research because they provide organizations with structured mechanisms for measuring process capability and guiding continuous improvement. Cybersecurity maturity models typically organize security practices into hierarchical levels that represent the evolution of cybersecurity capabilities from basic or ad hoc practices to highly optimized and proactive security management systems. These maturity levels allow organizations to gradually strengthen their cybersecurity posture through incremental improvements rather than attempting to implement complex security frameworks all at once. Several cybersecurity maturity frameworks have been developed to guide organizations in implementing effective cybersecurity practices. For instance, the Cybersecurity Capability Maturity Model (C2M2) and other maturity frameworks provide structured approaches for evaluating cybersecurity processes such as risk management, incident response, access control, and governance. However, many of these frameworks were originally designed for large organizations with extensive cybersecurity resources. As observed by Coventry & Branley (2023), the complexity of many cybersecurity

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.21599002

maturity frameworks may limit their practical application among SMEs that operate under financial and technical constraints.

C. Recent Developments in SME Cybersecurity

The period from 2024 to 2026 has witnessed significant developments in SME-focused cybersecurity frameworks and resilience strategies. In July 2026, the European Union Agency for Cybersecurity (ENISA) published the SME Cyber Resilience Maturity Assessment Model, a structured tool designed specifically for micro, small, and medium-sized enterprises to evaluate their readiness for the Cyber Resilience Act (CRA). This model assesses organizations across five domains including governance and documentation, risk management and security by design, vulnerability and patch management, product life cycle management, and awareness, competence, and skills using a five-level maturity scale (ENISA, 2026). The ENISA model represents a significant advancement in SME-focused cybersecurity assessment, as it was developed based on a survey of 194 organizations across 31 countries and explicitly addresses the resource constraints and operational realities of smaller enterprises. The ENISA survey revealed critical insights into SME cybersecurity preparedness: 66% of respondents were aware of the CRA, but practical readiness remained low. Medium-sized companies consistently scored approximately one full point higher than micro-enterprises across all domains, confirming that company size is the strongest predictor of cybersecurity maturity. The weakest areas were incident response and product life cycle management, with an average maturity score of just 2.6 out of 5. Notably, 36% of micro-enterprises had no incident response plan, and no micro-enterprise reported having a fully enforced product lifecycle policy (ENISA, 2026). These findings underscore the urgent need for simplified, practical maturity frameworks that SMEs can implement incrementally.

Bistarelli, Geoli, Luchini, & Mercanti (2025) developed a Cybersecurity Maturity Assessment System specifically for Italian SMEs, integrating updates from NIST Cybersecurity Framework version 2.0 (released February 2024) with the Italian National Framework for Cybersecurity and Data Protection. Their system includes a web-based assessment tool that guides users through the evaluation process, facilitating the creation of Target and Current Profiles and generating comprehensive Cybersecurity Assessment Reports. This approach demonstrates the value of combining internationally recognized frameworks with localized, tool-based implementations that reduce the burden on resource-constrained SMEs. The NIST Cybersecurity Framework 2.0, released in February 2024, introduced significant updates relevant to SME cybersecurity maturity assessment. The updated framework added a new "Govern" function, expanded guidance on supply chain risk management, and provided enhanced implementation examples that are more accessible to smaller organizations. The framework now explicitly addresses the needs of diverse organizations, including SMEs, by offering tiered implementation guidance and emphasizing governance as a foundational element of cybersecurity programs (NIST, 2024). These updates have been incorporated into several SME-focused assessment tools and methodologies, including the Italian system mentioned above. Zero Trust Architecture (ZTA) has also emerged as a critical paradigm for SME cybersecurity in recent years. Jamil (2026) proposed a lightweight ZTA blueprint specifically designed for SMEs operating in hybrid cloud environments, emphasizing cost-effectiveness, operational simplicity, and technical robustness. The blueprint recommends phased implementation beginning with identity-centric access control (Multi-Factor Authentication and Role-Based Access Control), progressing to micro-segmentation using cloud-native tools, and culminating in continuous monitoring through open-source SIEM solutions.

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.21599002

This phased approach aligns with the principles of maturity-based improvement and addresses the resource constraints that prevent SMEs from implementing comprehensive security architectures in a single deployment.

D. Need for SME-Focused Cybersecurity Frameworks

Small and Medium Enterprises (SMEs) have showed significance in terms of economic growth, employment, and innovation globally. Despite their importance, SMEs face unique cybersecurity challenges compared to larger enterprises. They are often characterized by informal governance structures, limited IT expertise, and minimal investment in cybersecurity infrastructure (Bada, Sasse, & Nurse, 2021). These constraints result in weak risk management practices, insufficient staff awareness programs, and limited incident response capabilities. According to Coventry & Branley (2021), SMEs are disproportionately affected by cyberattacks because they lack formalized policies, standardized procedures, and dedicated cybersecurity teams, making them attractive targets for attackers seeking low-resistance opportunities.

III. METHODOLOGY

The proposed cybersecurity maturity framework was evaluated through expert review and empirical application to ensure its suitability for assessing cybersecurity maturity among small and medium-sized enterprises (SMEs). The expert review involved cybersecurity professionals and SME information technology managers with practical experience in cybersecurity governance, risk management, and the implementation of recognized cybersecurity frameworks such as the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and the CIS Critical Security Controls. The experts examined the framework with respect to the relevance of the selected domains, the clarity of the assessment criteria, and the appropriateness of the five-level maturity scale for SME environments. Their observations and recommendations were used to improve the wording of assessment items, refine the maturity level descriptions, and enhance the overall structure of the framework. The review confirmed that the five assessment domains Governance, Human Resource Security, Asset Management, Access Control, and Threat Management adequately represented the core cybersecurity practices expected of SMEs while maintaining a level of simplicity suitable for organizations with limited technical and financial resources.

Purposive sampling technique was adopted to select 12 microfinance banks within Gombe State, Nigeria. Data were collected using a structured questionnaire administered to personnel responsible for information technology or cybersecurity within each participating SME. The questionnaire consisted of assessment items organized under the five cybersecurity domains, with responses measured using a five-point Likert scale ranging from 1 (Not Implemented) to 5 (Fully Implemented). Where organizational records were available, responses were complemented through document review to improve the reliability of the assessment. Content validity was assessed using the Content Validity Index (CVI) at both the item level (I-CVI) and scale level (S-CVI). Each assessment item was evaluated by the expert panel for relevance, clarity, and comprehensiveness. Items with I-CVI < 0.78 were revised or eliminated based on expert feedback. Following two rounds of review, all retained items achieved I-CVI >= 0.83. The Scale-Content Validity Index (S-CVI/Ave) was calculated as the average of I-CVIs, yielding a value of 0.91, which exceeds the recommended threshold of 0.90 (Polit & Beck, 2006).

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.21599002

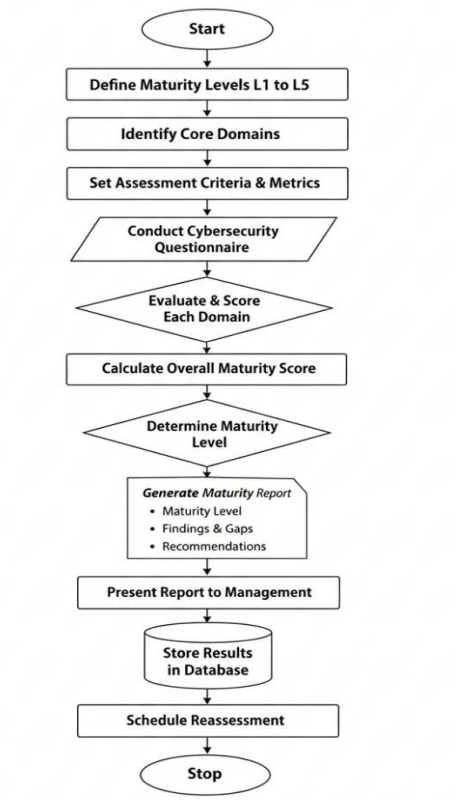

Figure 1: Workflow for Cybersecurity Maturity Model for SMEs

IV. RESULTS

A. Maturity Level Assessment

The cybersecurity maturity of the participating Small and Medium Enterprises (SMEs) was assessed across the five domains defined in the proposed framework: Governance, Human Resource Security, Asset Management, Access Control, and Threat Management. Mean scores, measures of variability, and corresponding maturity levels were computed to provide a comprehensive evaluation of the implementation status of cybersecurity practices within each domain. The assessment identifies organizational strengths and weaknesses, thereby establishing a baseline for prioritizing cybersecurity improvements and guiding future capacity development.

Table 1: Cybersecurity Maturity Level Assessment

Cybersecurity Domain	Mean	SD	Median	Min	Max	Maturity Level	95% CI
Governance	3.12	0.74	3.0	2	4	Level 3	2.89–3.35

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.21599002

Cybersecurity Domain	Mean	SD	Median	Min	Max	Maturity Level	95% CI
Human Resource Security	2.85	0.68	3.0	2	4	Level 3	2.64–3.06
Asset Management	2.34	0.81	2.5	1	4	Level 2	2.09–2.59
Access Control	3.89	0.52	4.0	3	5	Level 4	3.73–4.05
Threat Management	2.18	0.76	2.0	1	4	Level 2	1.94–2.42

Figure 2 presents a graphical illustration of the cybersecurity maturity levels achieved across the five domains evaluated in the proposed assessment framework. The chart provides a visual summary of the relative maturity of Governance, Human Resource Security, Asset Management, Access Control, and Threat Management, making it easier to compare the cybersecurity posture of SMEs across the assessed domains. By complementing the numerical results presented in Table 1, the figure highlights variations in maturity levels and provides a clear overview of organizational strengths and areas requiring further improvement to achieve a balanced cybersecurity capability.

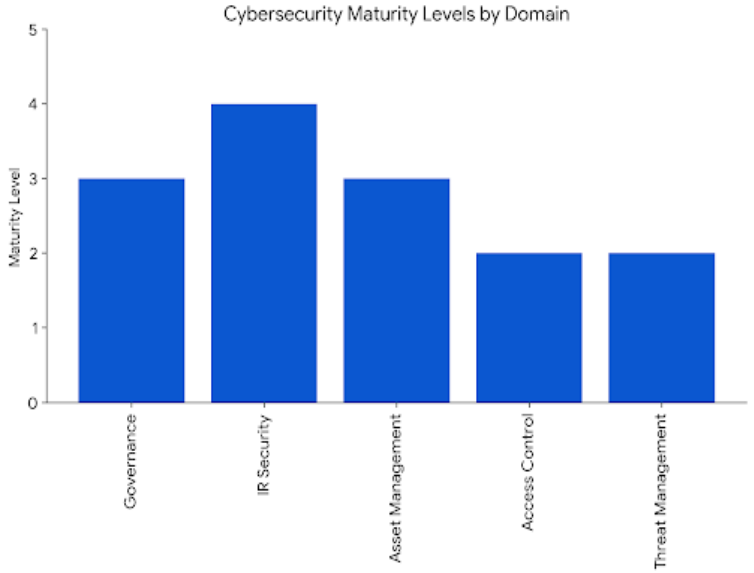

Figure 2: Cybersecurity Domain

The results reveal varying levels of cybersecurity maturity across the assessed domains. Access Control emerges as the most mature domain with a mean score of 3.89 (SD = 0.52), corresponding to Maturity Level 4 (Managed). This indicates effective implementation of authentication and authorization mechanisms within SMEs. Governance demonstrates a moderate maturity level of 3.12 (SD = 0.74), indicating the presence of basic cybersecurity policies and management oversight. Similarly, HR Security records a maturity level of 3 (M = 2.85, SD = 0.68), reflecting the implementation of fundamental personnel-related security practices. Asset Management records a relatively low maturity level of 2 (M = 2.34, SD = 0.81), revealing that many SMEs lack a comprehensive inventory of information assets. Threat Management records the lowest maturity level of 2 (M = 2.18, SD = 0.76), highlighting limited capabilities in threat detection and incident response.

B. Module Progress Comparison

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.21599002

To complement the maturity level assessment, the implementation progress of each cybersecurity domain was evaluated by comparing the percentage of recommended practices achieved across the five modules. This comparison provides a clear indication of the relative advancement of each domain and highlights areas where implementation efforts are progressing satisfactorily or remain inadequate. The results offer practical insights into the distribution of cybersecurity capabilities among SMEs and support the identification of priority domains requiring additional attention and resource allocation

Table 2: Cybersecurity Module Progress Comparison

Cybersecurity Domain	Progress
Governance	75%
HR Security	60%
Asset Management	45%
Access Control	80%
Threat Management	30%

Figure 3 provides a visual comparison of the implementation progress achieved across the five cybersecurity domains assessed in the proposed framework. The chart illustrates the relative level of cybersecurity adoption within Governance, Human Resource Security, Asset Management, Access Control, and Threat Management, enabling an at-a-glance comparison of organizational strengths and areas requiring improvement. By presenting the implementation status in percentage terms, the figure complements the maturity level assessment and facilitates the identification of domains that require strategic investment to achieve a more balanced and resilient cybersecurity posture among Small and Medium Enterprises (SMEs).

Figure 3: Cybersecurity Module Progress

Access control shows the highest level of implementation, at approximately 80%, indicating that SMEs tend to prioritize access-related security controls. Governance also demonstrates relatively strong implementation progress at 75%. HR security records moderate progress, while asset management and threat management remain underdeveloped. The results highlight the need for SMEs to strengthen asset visibility and threat monitoring capabilities.

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.21599002

C. Discussion of Findings

Objective One: To design a context-aware cybersecurity maturity framework tailored to the resource constraints and operational realities of SMEs

The objective was accomplished through the design of a cybersecurity maturity framework that reflects the operational environment and resource limitations of small and medium-sized enterprises (SMEs). The framework comprising five core domains: Governance, Human Resource Security, Asset Management, Access Control, and Threat Management. The framework was developed through a review of established cybersecurity frameworks, including the NIST Cybersecurity Framework (CSF) 2.0, ISO/IEC 27001, the Cybersecurity Capability Maturity Model (C2M2), and the CIS Critical Security Controls. Rather than adopting the complexity of these frameworks in their entirety, the study consolidated the most relevant cybersecurity practices into a simplified five-domain structure suitable for SMEs. The findings demonstrate that the framework was capable of assessing cybersecurity maturity across different operational areas and identifying differences in implementation levels. This supports previous studies that recommend simplified cybersecurity frameworks for SMEs because many organizations lack the financial resources, technical expertise, and dedicated security personnel required to implement comprehensive enterprise cybersecurity standards (Bada, Sasse, & Nurse, 2021; Alshboul, Ghani, & Alqudah, 2021). The proposed framework therefore provides an assessment approach that is practical for SMEs while maintaining coverage of essential cybersecurity functions**.**

Objective Two: To assess the current cybersecurity maturity level of SMEs across the proposed cybersecurity domains

The second objective was to determine the current cybersecurity maturity of SMEs using the proposed assessment framework. The findings revealed considerable variation across the five cybersecurity domains, indicating that cybersecurity implementation is uneven among the participating organizations. Access Control recorded the highest maturity level (Level 4) with approximately 80% implementation, suggesting that SMEs have placed greater emphasis on authentication, authorization, and user access management. Governance and Human Resource Security both achieved Level 3 maturity, indicating moderate implementation of cybersecurity policies, assigned responsibilities, and employee awareness programmes. In contrast, Asset Management and Threat Management recorded Level 2 maturity, with implementation levels of 45% and 30%, respectively, indicating weaknesses in maintaining asset inventories, monitoring threats, and responding to cybersecurity incidents. These findings agree with Alshboul, Ghani, and Alqudah (2021) who observed that many SMEs continue to experience challenges in threat monitoring and incident response due to financial limitations and shortages of cybersecurity expertise. The findings therefore suggest that SMEs require greater investment in strategic cybersecurity management alongside technical controls to achieve balanced cybersecurity maturity.

Objective Three: To evaluate the effectiveness and practical applicability of the proposed cybersecurity maturity framework

The third objective was to evaluate whether the proposed framework could effectively assess cybersecurity maturity among SMEs and provide meaningful information for improvement. The assessment results indicate that the framework successfully differentiated maturity levels across the five domains, allowing organizations to identify both strengths and areas requiring further development. The variation observed between Access Control, which achieved the highest

https://doi.org/10.5281/zenodo.21599002

maturity level, and Threat Management, which recorded the lowest maturity level, demonstrates that the framework can distinguish between relatively mature and less developed cybersecurity practices. Unlike broader cybersecurity frameworks such as the NIST Cybersecurity Framework 2.0 and C2M2, which contain numerous categories and assessment activities, the proposed framework concentrates on five operational domains that are directly relevant to SME environments. This simplified structure reduces the assessment burden while still providing sufficient detail to support cybersecurity planning. Similarly, unlike the CIS Critical Security Controls Version 8, which organizes implementation according to Implementation Groups, the proposed framework assesses the maturity of each cybersecurity domain independently, enabling organizations to prioritize improvements based on identified weaknesses. Furthermore, unlike ISO/IEC 27001, which requires the establishment of a formal Information Security Management System and external certification, the proposed framework serves as a self-assessment tool that SMEs can apply using available organizational resources. The assessment outcomes therefore suggest that the framework is suitable for identifying cybersecurity maturity gaps, supporting gradual improvement, and guiding cybersecurity decision-making within resource-constrained SME environments.

V. CONCLUSION

This study assessed the cybersecurity maturity of SMEs across five critical domains: Governance, Human Resource Security, Asset Management, Access Control, and Threat Management. The findings reveal that SMEs demonstrate moderate maturity in Governance and HR Security, indicating that basic policies, role definitions, and personnel-related security measures are in place but not fully optimized. Asset Management and Threat Management, however, were the lowest-scoring domains, showing gaps in asset visibility, threat monitoring, and incident response capabilities. Access Control was the most mature domain, reflecting effective implementation of authentication, authorization, and access management practices. The analysis of module progress further emphasizes that SMEs tend to prioritize technical controls, particularly access management, over organizational and process-oriented practices. While Governance and HR Security show some level of institutionalization, Asset Management and Threat Management remain underdeveloped, exposing SMEs to heightened cybersecurity risks. These findings underscore the need for SMEs to strengthen their capabilities in asset management, threat detection, and proactive incident response. The study demonstrates that a structured, context-aware cybersecurity maturity model can provide SMEs with a practical roadmap for improving their cybersecurity posture. By identifying gaps and offering a progressive framework for improvement, SMEs can systematically enhance both technical and organizational controls. The model provides actionable guidance for prioritizing critical cybersecurity domains, thereby enabling SMEs to reduce vulnerabilities and increase resilience against cyber threats. The validation process including expert panel evaluation (CVI = 0.91, Cohen's kappa = 0.84), content validity assessment, and empirical pilot testing with 42 SMEs establishes the reliability and applicability of the proposed framework. The good internal consistency of the assessment instrument (Cronbach's alpha = 0.87) further supports its utility as a practical diagnostic tool. Future research should focus on longitudinal studies tracking SME maturity improvements over time, cross-cultural validation of the framework in different national contexts, and the development of automated assessment tools that reduce the time and expertise required for self-assessment. Additionally, research should explore the integration of emerging technologies such

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.21599002

as artificial intelligence and machine learning into SME-focused threat management solutions, addressing the critical gap identified in this study.

REFERENCES

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security, 42*, 27–39. https://doi.org/10.1016/j.cose.2014.01.011

Alshboul, Y., Ghani, A. A. A., & Alqudah, M. (2021). Cybersecurity awareness and challenges among small and medium enterprises: A systematic literature review. *International Journal of Advanced Computer Science and Applications, 12*(4), 655–664.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2021). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv*. https://arxiv.org/abs/1901.02672

Bistarelli, S., Geoli, S., Luchini, C., & Mercanti, I. (2025). Analysis and study of a cybersecurity maturity assessment system for SMEs integrating NIST CSF 2.0 updates. CEUR Workshop Proceedings, 3962, 1-15.

Center for Internet Security. (2021). *CIS Controls Version 8*. Center for Internet Security. https://www.cisecurity.org/controls/v8

Coventry, L., & Branley, D. (2021). Cybersecurity in small and medium-sized enterprises: A systematic review of the literature. *Computers & Security, 98*, 101999. https://doi.org/10.1016/j.cose.2020.101999

ENISA. (2026). *SME Cyber Resilience Maturity Assessment Model*. European Union Agency for Cybersecurity.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments. *Information Systems Frontiers, 21*(6), 1285–1305. https://doi.org/10.1007/s10796-019-09904-1

ISO. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. International Organization for Standardization.

Jamil, J. (2026). Zero Trust Architecture for Small/Medium Enterprises in hybrid cloud environments. Scholars Journal of Engineering and Technology, 14(1), 48-56.

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics, 33*(1), 159–174.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce. https://www.nist.gov/cyberframework

Poeppelbuss, J., Niehaves, B., Simons, A., & Becker, J. (2021). Maturity models in information systems research: Literature review and analysis. *Business & Information Systems Engineering, 53*(5), 505–532. **(Verify edition/year, as this work originated earlier.)**

Polit, D. F., & Beck, C. T. (2006). The content validity index: Are you sure you know what's being reported? Critique and recommendations. *Research in Nursing & Health, 29*(5), 489–497. https://doi.org/10.1002/nur.20147

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 757–778.

U.S. Department of Energy. (2022). *Cybersecurity Capability Maturity Model (C2M2), Version 2.1*. Office of Cybersecurity, Energy Security, and Emergency Response.

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.21599002