Comparative Analysis of Small and Medium-Sized Enterprises Cybersecurity Program Assessment Model

Wan Nur Eliana Wan Mohd Ludin[1], Masnizah Mohd[2], Wan Fariza Paizi@Fauzi[3]
Center for Cyber Security-Faculty of Information Science & Technology,
Universiti Kebangsaan Malaysia, Bangi, Selangor Malaysia[1, 2, 3]
Faculty of Computer Science and Information Computing Technology,
New Era University College, Kajang, Selangor, Malaysia[1]

***Abstract*—In the digital age, Small and Medium-sized Enterprises must review and improve their cybersecurity posture to combat rising risks. This paper thoroughly compares Small and Medium-sized Enterprises cybersecurity program assessment approaches. The National Institute of Standards and Technology's Cybersecurity Framework, CyberSecurity Readiness Model for SMEs, Cybersecurity Evaluation Model, and Adaptable Security Maturity Assessment and Standardisation framework were examined. The NIST CSF is adaptable and applicable to many sectors, while the CSRM provides a standardized way to assess an organization's cyber readiness. With its resource limits and operational scales, the CSRM-SME meets SMEs' particular issues. Organizations may examine and improve cybersecurity with CSEM. The approach can be used for SMEs, higher education institutions, and industrial control systems. The ASMAS architecture is flexible for continual security enhancement due to its scalability and standardization. This comparison analysis shows each framework's strengths and weaknesses, revealing their suitability for diverse SME scenarios. This paper helps SMEs choose the best model to strengthen cybersecurity, boost resilience, and meet global standards. This paper will compare the NIST CSF, CSRM-SME, CSEM, and ASMAS cybersecurity frameworks.**

***Keywords*—Cybersecurity; SMEs; cybersecurity program assessment models; cybersecurity assessment frameworks**

I. Introduction

Small and Medium-sized Enterprises (SMEs) are vital to the economy but are frequent targets of cyberattacks due to their limited cybersecurity capabilities [1]. Existing maturity assessment models and standards often need to pay more attention to SMEs' requirements and roles in the digital ecosystem. The rise of Industry 4.0 and digital transformation introduces new cybersecurity challenges for SMEs. A tailored cybersecurity assessment model is needed to address the unique cybersecurity needs of SMEs. This model should consider SMEs' resources and expertise limitations while providing effective cybersecurity measures [2].

A. Global and Malaysia Small and Medium-sized Enterprises (SMEs)

SMEs drive innovation, competitiveness, and job creation, making them the backbone of the economy [3]. These companies have fewer than 250 people and a turnover or balance sheet of less than €50 million or €43 million [4]. Most countries have SMEs, including 99% of EU enterprises [5]. SMEs boost GDP, employment, and innovation, making them crucial to the economy. SMEs provide half of U.S. jobs but only 40% of GDP [6]. SMEs comprise 98% of Australian enterprises, contribute one-third of GDP, and employ 4.7 million people. SMEs generate 44% of Norway's economic value and employ 47% of private sector workers [7].

Malaysia's SMEs boost GDP, employment, and innovation. SME definitions include sales turnover and full-time employee count. SME status in Malaysia is determined by a sales turnover of RM50 million or fewer than 200 full-time employees [8]. Malaysian SMEs are classified by sales turnover and full-time personnel. Micro, small, and medium requirements, such as manufacturing and services, vary by industry. The manufacturing sector has microenterprises with sales turnovers under RM300,000 or less than five full-time employees. However, a tiny business makes between RM300,000 and RM15 million [9].

The Malaysian economy relies on SMEs, which comprise 97.2% of businesses, 38.2% of GDP, and 7.3 million jobs. These businesses generate economic growth, with 98.5% of Malaysian companies being SMEs. SMEs generated about RM500 billion to Malaysia's GDP and 5.7 million jobs, 70% of the workforce in 2018. [10]. To keep up with digital culture, SMEs should use digital marketing to boost market presence and efficiency. The government helps SMEs digitalize to expand their consumer base and increase efficiency. Establishing the Ministry of Entrepreneur Development and Cooperatives (MEDAC) shows the government's support for SMEs and entrepreneurship. The National Entrepreneur and SME Development Council (NESDC) promotes entrepreneurship to boost economic growth [11].

Table I compares Small and Medium-sized Enterprises (SMEs) globally and SMEs, specifically in Malaysia, across various aspects, including economic contribution, internationalization, technology adoption, government support, market orientation, challenges, performance factors, environmental practices, and corporate governance. The importance of SMEs globally and in Malaysia while also showcasing the unique challenges they face and the support systems in place to help them thrive. It underscores the critical

role of policy measures and innovation in driving SME growth and sustainability.

TABLE I. COMPARISON OF GLOBAL SMES AND MALAYSIA SMES

Criteria	Global SMEs	Malaysia SMEs
Economic Contribution [3]	Significant contribution to GDP and employment across various countries.	Manage 98.5% of Malaysian businesses, 65.3% of jobs, and 36.3% of GDP.
Internationalization (4)	We are engaged in global markets through exports, joint ventures, and international partnerships.	Exports boost GVC and FTA participation.
Technology Adoption [5]	Adoption varies widely; advanced economies often lead to technology integration.	High expenses and the need for innovation to stay competitive hinder technology adoption.
Government Support [6]	Various support levels, including financial aid, training, and internationalization assistance.	Significant government development, financial, and export promotion support.
Market Orientation [7]	Market orientation is critical for success; firms focusing on customer needs and market trends perform better.	Customer attention and market dispersion are essential, but intelligence and reactivity differ.
Challenges [8]	Common challenges include access to finance, competition, and regulatory hurdles.	Lack of competent labor, high raw material costs, and upfront investment costs.
Performance Factors [9]	Performance is linked to innovation, market expansion, and efficient resource utilization.	Internationalization and performance are linked, emphasizing market orientation.
Environmental Practices [8]	Increasing emphasis on sustainability and green practices in developed countries.	Early green practices; ISO 14001 Environmental Management System to improve performance.
Corporate Governance [10]	Varies significantly; better corporate governance practices are correlated with improved SME performance.	Better corporate governance practices are needed for monitoring and procedure implementation.

II. BACKGROUND ASSESSMENT MODELS AND FRAMEWORKS

An organization's security posture can be assessed and improved using a cybersecurity program assessment model to discover vulnerabilities, assess risks, and deploy controls. These models evaluate external threats like cyberattacks and internal weaknesses like obsolete software or human errors that could affect an organization's information systems [11]. They include methods for estimating and prioritizing risks, assessing cyber threat impact and likelihood, and selecting reaction levels [12]. These models help organizations establish security policies, access controls, firewalls, and personnel training to limit risks [13]. As threats change, effective cybersecurity program assessment models emphasize continual monitoring and periodic appraisal to improve the organization's cybersecurity posture [14]. Numerous models link with international standards like ISO/IEC 27001 and 27002, offering a benchmark for cybersecurity maturity and compliance [15]. Cybersecurity program assessment models help organizations prepare for growing cyber threats with these comprehensive techniques.

A. Taxonomy Assessment Models

Cybersecurity program assessment models are diverse frameworks designed to evaluate and enhance the security posture of organizations. These models systematically categorize different aspects of cybersecurity to provide a comprehensive and structured approach to risk assessment, threat identification, and mitigation. The taxonomy of these models often includes various components such as risk factors, threat vectors, control measures, and evaluation criteria.

TABLE II. THE SUMMARY TAXONOMY ASSESSMENT MODEL

Taxonomy	Description
Risk-Based Taxonomy	Risk identification, analysis, and management. Quantifies threat occurrences, vulnerability, and effect of cybersecurity threats. Quantitative algorithms measure cybersecurity risk using these parameters [11].
Hierarchical and Graph-Theoretic Taxonomy	Uses hierarchical and graph-theoretic models to assess cybersecurity vulnerabilities. Taxonomically classifies threat actors' methods and provides cyber-physical assault graphs to analyze threat transmission [12].
Capability Maturity Models (CMMs)	Assess and improve an organization's cybersecurity. Classifies maturity levels in policy, operations, and human factors. Compares the present situation to optimal practices [13].
Socio-Technical Taxonomy	Assesses cybersecurity threats and improves IT, security, and non-technical staff communication using technical and human factors. Work processes and hazards are visualized using modeling languages [14].
Multicriteria Decision Frameworks	Integrates various criteria to assess the overall utility of cybersecurity management alternatives. Quantifying threats, vulnerabilities, and consequences provides a structured approach to selecting risk management actions [15].
Dynamic Simulation-Based Taxonomy	Assesses cybersecurity threats and plans long-term investments using dynamic simulation. Addresses organizational change and cyberattack dynamics [16].
Comprehensive and Flexible Taxonomies	Includes worldwide and national cybersecurity recommendations. Technology, organization, people, and environment are measured to assess cybersecurity readiness [17].

Organizational security is assessed and improved using several cybersecurity program assessment methodologies. These frameworks categorize cybersecurity to organize risk assessment, threat identification, and mitigation. Table II shows that these models' taxonomies comprise risk variables, threat vectors, control measures, and evaluation criteria.

Several taxonomic techniques are used to control and reduce cybersecurity threats. Risk-based taxonomies categorize risks into quantifiable criteria, including attack events, vulnerabilities, and impacts, and employ quantitative algorithms to evaluate and prioritize cybersecurity risks [11]—however, hierarchical and graph-theoretic taxonomies model cybersecurity concerns. Taxonomical classifications of threat actors' approaches, tactics, and processes generate cyber-physical attack graphs that analyze threat propagation, helping identify vital assets and prioritize controls [12]. CMMs evaluate and improve an organization's cybersecurity practices in policy, operations, and human factors. The National Cybersecurity Capacity Maturity Model (CMM) lets organizations compare their current condition to best

practices and identify areas for improvement [17]. Multicriteria decision frameworks quantify threats, vulnerabilities, and consequences to evaluate cybersecurity management alternatives and provide a structured approach for risk management action selection, bridging the gap between risk assessment and risk management [15]. Comprehensive and flexible taxonomies include worldwide and national cybersecurity recommendations for technology, organizations, people, and the environment. These holistic cybersecurity readiness models are adaptable to organizational situations [17].

B. Process Development Assessment Model

Developing a cybersecurity program assessment model involves a structured and iterative process to evaluate and enhance an organization's cybersecurity posture. This structured and iterative process ensures that organizations can systematically assess, manage, and strengthen their cybersecurity posture, thereby reducing risks and improving overall security resilience.

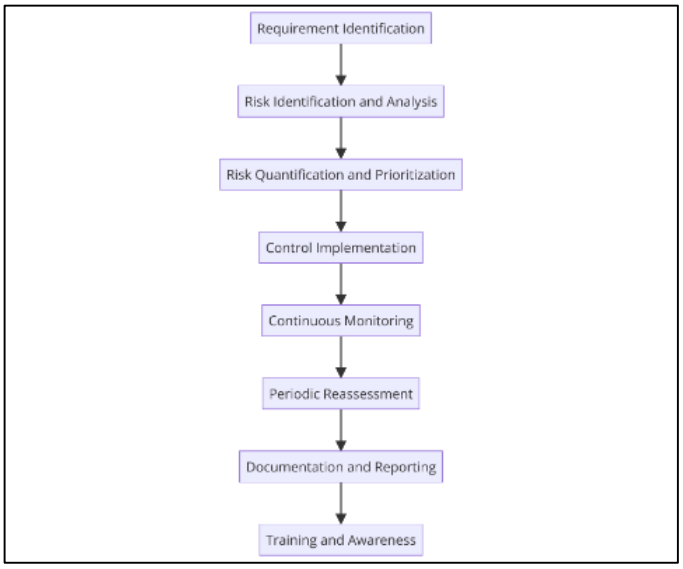

Fig. 1. Process of developing assessment model.

Fig. 1 demonstrates an organization's comprehensive cybersecurity management procedure. It starts with need identification, which defines cybersecurity needs, limitations, behaviors, services, and security requirements [18]. Next, Risk Identification and Analysis involves detecting and analyzing internal and external cybersecurity risks and understanding threats and vulnerabilities [19]. After that, risk quantification and prioritization are employed to assess and rank these risks by impact and likelihood [15]. Control Implementation involves creating and implementing security policies, access controls, and employee training programs to reduce these risks [20]. Continuous Monitoring ensures these measures are effective through audits, vulnerability scans, and real-time threat detection. Reassessment and control adjustments are made to handle

C. Paper Structure

This paper will compare these cybersecurity frameworks, focusing on the NIST CSF, CSEM, CSRM-SME, and ASMAS. By examining their structures, implementation processes, strengths, weaknesses, and suitability for different organizational contexts, this paper provides insights into the most effective strategies for enhancing cybersecurity readiness, particularly for SMEs. Through this comparison, we aim to highlight each framework's key features and benefits, ultimately guiding organizations in selecting the most appropriate framework for their cybersecurity needs.

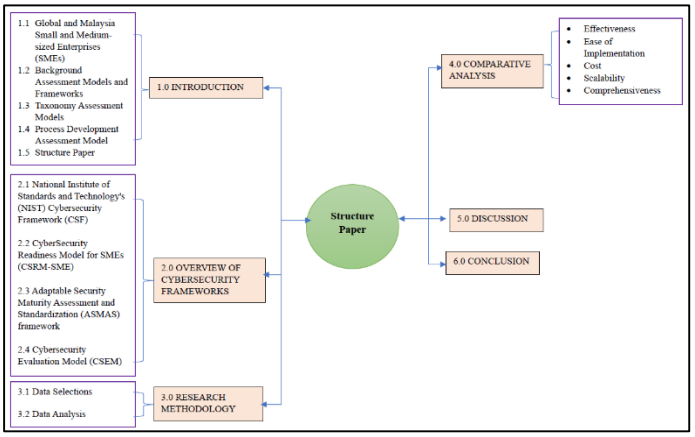

Fig. 2. The structure of the paper.

The structure of this paper is outlined in Fig. 2. Section I discusses an introduction to SMEs and the background of assessment models and frameworks. Section II discusses an overview of the cyber security model and framework. Section III discusses the research methodology. Then, Section IV presents the comparative analysis of cybersecurity program assessment models and frameworks. Finally, this paper presents the discussion and conclusions in Sections V and VI respectively.

III. Cybersecurity Program Assessment Model

Cybersecurity has become a critical concern for Small and Medium-sized Enterprises (SMEs) in Malaysia, given the increasing sophistication and frequency of cyber threats. Developing and implementing a comprehensive cybersecurity program assessment model tailored for Malaysian SMEs is essential to enhance their resilience against cyberattacks.

ISO 27001, while a comprehensive and internationally recognized standard, is often resource-intensive, requiring significant financial and human resources to implement effectively. This can be a substantial barrier for SMEs, which typically operate with limited budgets and may need more specialized staff to manage such a complex framework [18], [19]. Furthermore, the flexibility of ISO 27001, while beneficial for large organizations with diverse needs, may result in an overly broad approach that aligns poorly with SMEs' specific and more narrowly focused security needs [20]. Similarly, while the CIS Controls are designed to be more accessible and prescriptive, they may still present challenges in prioritization and customization that are difficult for SMEs to navigate without expert guidance. Though beneficial for comprehensive coverage, the CIS framework's broad scope may need to be aligned with the limited operational scope of many SMEs, making it less practical compared to more targeted cybersecurity assessment models [21].

A. National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF)

To help organizations manage and decrease cybersecurity risks, the NIST Cybersecurity Framework (CSF) provides comprehensive recommendations and best practices. The CSF was first published in 2014 and updated multiple times, with CSF 2.0 released in February 2024. This cybersecurity methodology is flexible and reproducible for all sizes and sectors of organizations. The five essential functions—Identify, Protect, Detect, Respond, and Recover—provide a comprehensive overview of an organization's cybersecurity risk management [33]. The framework is versatile so that organizations can customize it. System components include Framework Core, Framework Implementation Tiers, and Framework Profiles. This thorough guide helps organizations manage and reduce cybersecurity risks. It is versatile and adaptive to the needs of diverse organizations, regardless of size, sector, or maturity.

TABLE III. COMPONENTS IN THE NIST CYBERSECURITY FRAMEWORK (CSF)

Component	Description
CSF Core	Govern, Identify, Protect, Detect, Respond, and Recover are its main functions. Each function has categories and subcategories that define cybersecurity management outcomes and actions. The "Identify" function manages assets, whereas the "Protect" function controls access [22].
Implementation Tiers	Four implementation tiers: Partial (Tier 1) to Adaptive (Tier 4). These tiers show how risk management and corporate goals influence cybersecurity procedures. Higher tiers reflect more sophisticated cybersecurity risk management [22] [23].
Profiles	Custom framework implementations for unique organizations. They match cybersecurity with business needs, risk tolerance, and resources. Profiles help organizations prioritize and handle cybersecurity [22] [23].

Table III provides a concise overview of the critical components within the NIST Cybersecurity Framework (CSF). The paper overviews the framework's main elements, including CSF Core, Implementation Tiers, and Profiles. It emphasizes the significance and function of these components within the framework. Each component briefly describes how it contributes to aligning cybersecurity activities with organizational needs and risk management.

B. CyberSecurity Readiness Model- SME (CSRM-SME)

CSRM-SME is designed to enhance the cybersecurity posture of Small and Medium-sized Enterprises (SMEs) by addressing both technical and socio-technical dimensions. This model emphasizes the importance of balancing human and technical factors, fostering a strong cybersecurity culture, and using adaptable, metric-based assessments to address the unique challenges faced by SMEs [14].

Table IV shows that CSRM-SME provides a comprehensive approach to enhancing cybersecurity readiness by integrating socio-technical elements. This model emphasizes balancing human and technical factors, fostering a strong cybersecurity culture, and using adaptable, metric-based assessments to address SMEs' unique challenges. Implementing such a model can significantly improve SMEs' ability to manage cyber threats effectively.

TABLE IV. COMPONENT OF CSRM-SME

Core Component	Description
Socio-Technical Perspective	Assesses and improves cybersecurity readiness using human and technical factors. Focuses on organizational methods and technical defenses [14].
Human Element Integration	It maps socio-technical networks and human interactions using user journeys. It improves communication between IT, security, and non-technical staff to address human vulnerabilities [24].
Comprehensive Framework	Balances social, technical, and environmental factors. Provides a methodical approach to addressing SMEs' cybersecurity gaps [25].
Organizational Culture and Readiness	Highlights cybersecurity culture. It stresses that cybersecurity knowledge and culture are as necessary as technical solutions. Assesses essential areas for improvement [26].
Metric-Based Assessments	Reviews and creates socio-technical cybersecurity metrics. Addresses metric aggregation and flexibility for SMEs via straightforward, threat-based evaluations tailored to their needs [27].

C. Adaptable Security Maturity Assessment and Standardization (ASMAS) Framework

The Adaptable Security Maturity Assessment and Standardisation (ASMAS) framework has been examined in numerous studies to meet the cybersecurity needs of diverse organizations. SMEs face particular cybersecurity challenges; thus, a web-based ASMAS framework is proposed to handle them [25]. Another paper offers a European cybersecurity education maturity assessment methodology that defines knowledge units and standardizes instruction [25]. In contrast, [26] presents a maturity structure for Security Operation Centres (SOC) to ensure cybersecurity management. The research in [27] emphasizes adaptability and standardization by integrating cybersecurity maturity evaluations and standardization to satisfy organizational needs. Finally, the study in [28] proposes a security maturity self-assessment paradigm for the software development lifecycle to improve security. These numerous approaches demonstrate the need for adaptive frameworks to fulfill cybersecurity objectives across sectors and environments.

The Adaptable Security Maturity Assessment and Standardization (ASMAS) framework provides a comprehensive approach to enhancing cybersecurity practices within Small and Medium-sized Enterprises (SMEs). The framework is structured around three key aspects: core components, framework core, and implementation tiers, as shown in Table V. Following the framework, SMEs can systematically build a resilient security infrastructure that evolves with the changing threat landscape, thereby effectively safeguarding their operations and sensitive information.

TABLE V. SUMMARY CORE COMPONENT ASMAS FRAMEWORK

Aspects	Part	Descriptions
Core Components [29]	Risk Management	Identifying, assessing, and prioritizing risks.
	Security Policies	It establishes and enforces security policies and procedures.
	Access Control	Managing access to resources ensures that only authorized users can access sensitive information.
	Incident Response	I am preparing for and responding to security incidents.
	Continuous Monitoring	We regularly monitor security controls to detect and respond to new threats.
	Employee Training	We educate employees about best practices and protocols for security.
Framework Core [29]	Identify	It is understanding the business context, resources, and risk management processes.
	Protect	We are implementing safeguards to ensure the delivery of critical infrastructure services.
	Detect	Developing and implementing activities to identify the occurrence of a cybersecurity event.
	Respond	We are developing and implementing appropriate activities to take action regarding a detected event.
	Recover	It maintained plans for resilience and restored any impaired capabilities or services.
Implementation Tiers [29]	Tier 1: Partial	Informal and ad-hoc approaches to security.
	Tier 2: Risk-Informed	Awareness of risks and beginning to implement security measures systematically.
	Tier 3: Repeatable	We have established practices and policies for security management.
	Tier 4: Adaptive	Continuous improvement and adaptation to new threats.

D. Cybersecurity Evaluation Model (CSEM)

Organizations can examine and improve cybersecurity using the Cybersecurity Evaluation Model (CSEM). The approach can be used for SMEs, higher education institutions, and industrial control systems. Cybersecurity evaluation models (CSEM) research offers many risk assessment and management techniques. The study in [26] emphasize the COVID-19 pandemic's impact on cyber threats and the usage of Bayesian Networks, Random Forests, and Social Networks to assess cyber-attack risks. The study in [27] emphasizes threat modeling's strong ROI in spotting cyber threats and fixing design faults [26]. Construct a CSEM for Indian SMEs in a virtual team setting, highlighting the heightened cyber risk due to remote working during the pandemic and proposing a quantitative approach to analyze and mitigate these risks. Finally, a paper validating the CyberSecurity Audit Model (CSAM) in Canadian higher education institutions shows that CSAM can conduct comprehensive cybersecurity audits across domains, demonstrating its practicality and importance in improving cybersecurity [29] [30].

TABLE VI. CORE COMPONENTS CSEM

Component	Description
Risk Assessment	Assessing cybersecurity risks through surveys and identifying strengths and weaknesses [26].
Security Requirements	Establishing security requirements based on ISO/IEC 27002 standards [28].
Maturity Self-Assessment	Self-assessment of cybersecurity maturity using frameworks like NIST CSF [29].
Audit Model	A comprehensive model for conducting cybersecurity audits across various domains [30].
Risk Analysis and Mitigation	We integrate fault tree analysis and fuzzy decision theory for risk evaluation and mitigation [26].

Table VI shows the Cybersecurity Evaluation Model (CSEM) comprehensive framework designed to enhance organizations' cybersecurity posture through several vital components. The Risk Assessment component identifies strengths and weaknesses in an organization's cybersecurity posture by conducting detailed surveys. This is followed by Security Requirements, which establish baseline standards for cybersecurity measures based on recognized frameworks such as ISO/IEC 27002, ensuring that all necessary protocols are in place. Maturity Self-Assessment involves using frameworks like the NIST Cybersecurity Framework (CSF) to self-evaluate and improve cybersecurity practices across critical areas, including identification, protection, detection, response, and recovery. The Audit Model [36] component provides a structured approach for conducting thorough cybersecurity audits across various organizational domains, verifying the effectiveness of implemented controls. Finally, risk analysis and mitigation integrate advanced methods such as fault tree analysis and fuzzy decision theory to assess and mitigate cybersecurity risks, identify vulnerabilities, and develop strategies to address potential threats. These components form a robust model that helps organizations systematically manage and enhance their cybersecurity defenses.

E. Summary

The Adaptable Security Maturity Assessment and Standardization (ASMAS) framework and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) both aim to enhance cybersecurity practices but cater to different organizational needs. The ASMAS framework is specifically designed for Small and Medium-sized Enterprises (SMEs), offering a tailored, adaptable, and user-friendly approach that addresses the unique challenges faced by these smaller entities. In contrast, the NIST CSF is a comprehensive and flexible framework suitable for various organizations, including those in critical infrastructure sectors. Still, its complexity and resource demands can be challenging for smaller organizations to implement effectively. Ultimately, the choice between these frameworks should be guided by the organization's specific needs, resources, and capabilities.

The Cybersecurity Evaluation Model (CSEM) and the CyberSecurity Readiness Model for SMEs (CSRM-SME) both provide frameworks to enhance cybersecurity in Small and Medium-sized Enterprises (SMEs). Still, they cater to different organizational needs and complexities. The CSEM is designed to be practical and straightforward, focusing on assessing cybersecurity risks and providing clear guidelines for improvement, particularly in remote work environments. It utilizes a quantitative approach through surveys, making it accessible and easy to implement for SMEs looking to identify their cybersecurity strengths and weaknesses.

On the other hand, the CSRM-SME offers a comprehensive evaluation based on a socio-technical perspective, considering both technological and human factors. This model provides a holistic view of an organization's cybersecurity readiness by examining the interaction between technology, people, and processes. While it offers a deeper understanding of cybersecurity readiness, its implementation can be more complex and resource-intensive.

IV. Research Methodology

This paper employs a comparative research design to analyze and evaluate the effectiveness, implementation processes, and overall suitability of five distinct cybersecurity frameworks: the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), CyberSecurity Readiness Model for SMEs (CSRM-SME), and Adaptable Security Maturity, Assessment, and Standardization (ASMAS) framework.

A. Data Selection

Academic databases, industry reports, and framework documentation are secondary data sources. These resources explain framework structure, execution, and goals. Academic databases provide peer-reviewed research articles and studies for credibility and accuracy. Industry studies show how these frameworks are used through trends, applications, and expert analysis. However, framework documentation includes thorough implementation instructions and protocols. To ensure a comprehensive evaluation, consider these sources when selecting data. Integrating information from these varied sources helps create a complete grasp of each framework and enables an intense study of its practical and theoretical underpinnings. Fig. 3 shows the process data selection structure.

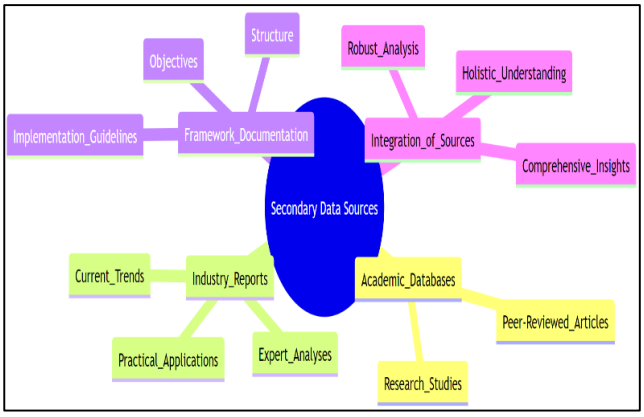

Fig. 3. Data selection structure.

B. Data Analysis

Comparisons of frameworks depend on literature and framework documentation content analysis. This method systematically analyses text to find patterns, themes, and critical traits. Analyzing academic articles, industry reports, and framework guidelines can reveal parallels and variances in framework structures, objectives, and implementation tactics. This technique helps compare frameworks and identify their strengths and drawbacks. Content analysis is a core method for organizing and synthesizing qualitative data into meaningful insights. This method ensures thorough research with empirical evidence, leading to more informed judgments and suggestions. Fig. 4 shows how content analysis compares framework stages and outcomes.

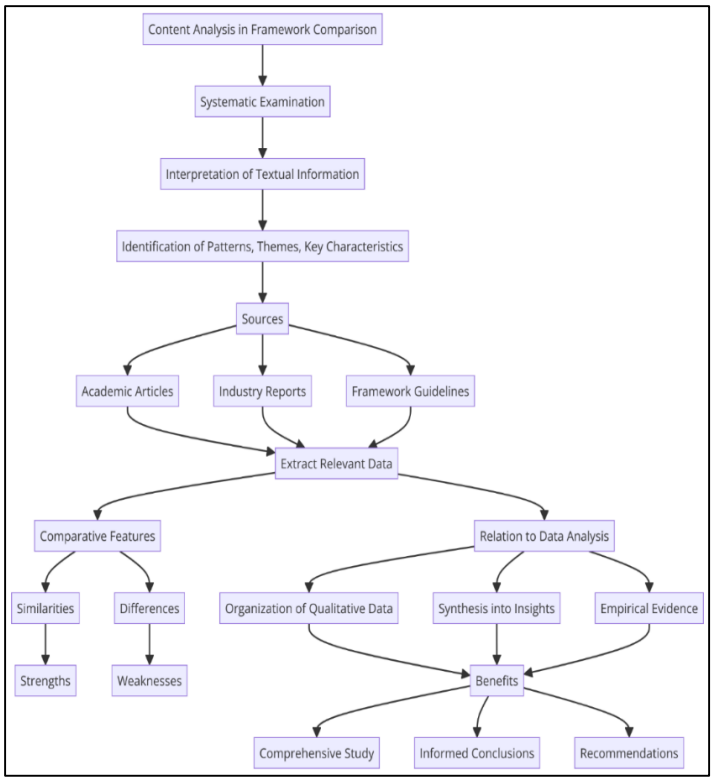

Fig. 4. Process of content analysis.

V. Result

In cybersecurity for Small and Medium-sized Enterprises (SMEs), a comparative analysis of various models is crucial to identify the most suitable framework. This analysis focuses on critical criteria: Effectiveness, Ease of Implementation, Cost, Scalability, and Comprehensiveness. The CyberSecurity Readiness Model for SMEs (CSRM-SME) is designed for small businesses, prioritizing ease of implementation and cost-effectiveness. The Cybersecurity Evaluation Model (CSEM) offers a robust framework emphasizing comprehensiveness and scalability, making it adaptable to various business sizes. The National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) is renowned for its effectiveness and comprehensiveness, providing a structured approach that is highly scalable but can be complex to implement for SMEs without significant resources. Lastly, the

Adaptable Security Maturity Assessment and Standardization (ASMAS) focuses on maturity and standardization, balancing comprehensiveness and ease of implementation while also being mindful of cost and scalability. This comparative analysis aims to elucidate the strengths and weaknesses of each model, helping SMEs choose the most appropriate framework for their specific needs and constraints.

Table VII above shows four highly effective and scalable models suitable for different SME needs. CSRM-SME, CSEM, and ASMAS stand out for their ease of implementation, while NIST CSF is noted for its comprehensive approach. Cost considerations vary, with CSEM and ASMAS being more affordable options.

Table VIII categorizes four cybersecurity models based on their performance across critical criteria. All frameworks are rated high for effectiveness, making them solid choices for enhancing cybersecurity. Regarding ease of implementation, CSRM-SME, CSEM, and ASMAS are rated high, indicating they are user-friendly and straightforward. In contrast, NIST CSF is rated moderate, requiring more effort for integration.

Cost-wise, CSEM and ASMAS are rated low, suggesting they are more affordable options, while CSRM-SME and NIST CSF are rated moderate. All frameworks are highly scalable and suitable for various organizational sizes and needs. Lastly, comprehensiveness is high for CSRM-SME, NIST CSF, and ASMAS, ensuring they cover a wide range of cybersecurity aspects, whereas CSEM is moderately comprehensive.

TABLE VII. COMPARATIVE ANALYSIS ASSESSMENT MODEL

Criterion	CSRM-SME [14]	CSEM [26]	ASMAS [29]	NIST Cybersecurity Framework (CSF) [27]
Effectiveness	The CSRM-SME model enhances cybersecurity readiness by integrating technical and human factors, providing a holistic and practical socio-technical approach.	CSEM provides a structured evaluation using a survey to assess cybersecurity risks, focusing on identifying strengths and weaknesses in SMEs' cybersecurity posture, which helps in targeted improvements	ASMAS addresses specific SME requirements for cybersecurity maturity and includes an evaluation study showing positive results for perceived usefulness and ease of use.	The NIST CSF offers a structured approach to managing cybersecurity risks and enhancing security posture across various sectors, including healthcare and financial services. Its core functions (Identify, Protect, Detect, Respond, Recover) provide comprehensive cybersecurity coverage.
Ease of Implementation	It uses a socio-technical approach, requiring comprehensive organizational changes, but is tailored for SMEs.	Utilizes an easy online survey for SMEs to complete, providing an accessible way to assess cybersecurity risks.	ASMAS is demonstrated through a web-based software prototype, showing ease of use and positive feedback from SMEs in evaluation studies	Implementing the NIST CSF can be complex and resource-intensive for SMEs, but it offers clear guidance and can integrate with other standards, enhancing ease of adoption.
Cost	The cost implications are not explicitly detailed but include potential expenses related to socio-technical adjustments within the organization.	CSEM involves minimal cost as it primarily uses a survey for self-assessment.	ASMAS uses a web-based software tool, which may involve initial setup costs but is designed for SMEs, keeping affordability in mind.	Implementing the NIST CSF can be costly due to technology, training, and maintenance investments. The Gordon-Loeb Model can help organizations evaluate cost-benefit aspects and optimize cybersecurity spending.
Scalability	The socio-technical approach can be scaled but might require tailored adjustments for different SME contexts.	It is scalable as it can be adapted for different SME sizes and industries by modifying the survey.	It is designed to be adaptable for various SMEs and includes specific adjustments to meet unique SME requirements, making it highly scalable.	The NIST CSF is scalable and adaptable, making it suitable for organizations of all sizes. It can be tailored to fit an organization's size, complexity, and cybersecurity needs.
Comprehensiveness	Comprehensive in addressing both technical and human aspects of cybersecurity readiness	Focuses on a comprehensive evaluation of cybersecurity maturity through detailed survey questions	Highly comprehensive, addressing both assessment and standardization needs specific to SMEs with positive evaluation results.	The NIST CSF is comprehensive, covering various cybersecurity areas with detailed guidelines. It aligns well with other standards, facilitating a holistic approach to managing cybersecurity risks.

TABLE VIII. EFFECTIVENESS PERFORMANCE

Criterion	CSRM-SME	CSEM	NIST CSF	ASMAS
Effectiveness	H	M	H	H
Ease of Implementation	M	H	M	H
Cost	M	L	M	M
Scalability	M	H	H	H
Comprehensive	H	M	H	H

H= High, M=Moderate, L= Low

VI. Discussion

The comparative analysis of the CyberSecurity Readiness Model for SMEs (CSRM-SME), Cybersecurity Evaluation Model (CSEM), National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), and Adaptable Security Maturity Assessment and Standardization (ASMAS) highlights the distinct strengths and focuses of each framework. All frameworks are recognized for their effectiveness in improving cybersecurity posture, making them well-regarded across various sectors. For instance, the CSRM-SME and ASMAS frameworks are particularly well-tailored for SMEs, effectively addressing their unique needs and constraints [14]. Similarly, the CSEM framework focuses on SMEs, emphasizing remote work environments, which have gained significant importance in the post-pandemic era [32]. On the other hand, the NIST CSF is noted for its comprehensiveness and widespread adoption across various industries, making it a robust choice for diverse organizational needs [34].

When considering ease of implementation, CSRM-SME, CSEM, and ASMAS stand out for their user-friendly guidelines and tools, facilitating straightforward adoption by SMEs. This high ease of implementation is supported by research highlighting these frameworks' design around SME constraints, such as limited resources and expertise [28]. In contrast, while the NIST CSF is effective, its broader scope and complexity may require more resources and expertise to integrate fully, especially within smaller organizations [31].

Cost is another critical factor, particularly for SMEs with limited budgets. Studies indicate that CSEM and ASMAS are cost-effective, making them accessible to smaller organizations [32]. Conversely, the CSRM-SME and NIST CSF are rated moderate in cost, as their implementation might require more extensive resources or adjustments, thereby incurring additional expenses [28].

In terms of scalability, all frameworks score high, reflecting their ability to adapt to organizations of different sizes and types. This scalability is essential for SMEs that may grow and require more comprehensive cybersecurity measures [32, 34]. Regarding comprehensiveness, the CSRM-SME, NIST CSF, and ASMAS frameworks are rated high as they cover a broad range of cybersecurity aspects and provide detailed guidelines for implementation. Meanwhile, CSEM, although practical, focuses primarily on remote working environments and best practices, making it less comprehensive in other cybersecurity [35] areas.

The findings underscore that while each cybersecurity framework is practical, their strengths and focus areas differ, making them suitable for varying organizational contexts. SMEs, in particular, can benefit from frameworks like CSRM-SME, CSEM, and ASMAS, specifically designed to address their unique needs and constraints.

VII. Conclusion

CSRM-SME and ASMAS are highly effective, easy to implement, comprehensive, and scalable, making them excellent choices for SMEs looking for robust, user-friendly cybersecurity solutions. They balance effectiveness and cost, ensuring that even smaller organizations can enhance their cybersecurity posture without significant financial strain. CSEM is also highly effective and cost-efficient, particularly suited for SMEs in remote working environments. It provides practical guidelines and tools, though it might not be as comprehensive in covering all cybersecurity aspects as other frameworks. NIST CSF stands out for its extensive and highly effective approach, suitable for various industries. However, implementing it may require more resources and expertise, which could be a consideration for smaller organizations with limited budgets.

Based on a comparative analysis of 4 cybersecurity models, the CyberSecurity Readiness Model for SMEs (CSRM-SME), the Cybersecurity Evaluation Model (CSEM), the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), and Adaptable Security Maturity Assessment and Standardization (ASMAS) the Adaptable Security Maturity Assessment and Standardization (ASMAS) emerges as the most suitable for SMEs.

ASMAS is highly effective in addressing the unique cybersecurity needs of SMEs, ensuring comprehensive coverage across various aspects of cybersecurity. Its high ease of implementation makes it accessible for SMEs lacking extensive cybersecurity expertise. Furthermore, ASMAS is cost-effective, an essential consideration for SMEs operating on limited budgets. The model's scalability ensures it can adapt and grow with the SME as its operations expand.

In conclusion, ASMAS provides a balanced and robust framework for SMEs to assess and enhance their cybersecurity posture, making it the most appropriate choice among the evaluated models. This framework will help SMEs manage their cybersecurity risks effectively, ensuring a secure and resilient digital environment.

References

[1] Fricker SA, Shojaifar A. Self-endorsed Cybersecurity Capability Improvement for SMEs. In: 28th Americas Conference on Information Systems. 2022.

[2] Yigit Ozkan B, Spruit M. Adaptable Security Maturity Assessment and Standardization for Digital SMEs. Journal of Computer Information Systems. 2023 Jul 4;63(4):965–87.

[3] Yusoff T, Wahab SA, Latiff ASA, Osman SIW, Zawawi NFM, Fazal SA. Sustainable Growth in SMEs: A Review from the Malaysian Perspective. Journal of Management and Sustainability. 2018 Aug 22;8(3):43.

[4] Arudchelvan M, Wignaraja G. SME Internationalization Through Global Value Chains and Free Trade Agreements: Malaysian Evidence. SSRN Electronic Journal. 2015.

[5] Kalesamy KM. A Conceptual Study: Technology Adoption among Malaysian Manufacturing SMEs for Corporate Sustainability in the Context of IR 4.0. The International Journal of Business & Management. 2021 Sep 30;9(9).

[6] Muhammad MZ, Char AK, Yasoa' MR bin, Hassan Z. Small and Medium Enterprises (SMEs) Competing in the Global Business Environment: A Case of Malaysia. International Business Research. 2009 Dec 15;3(1).

[7] Mokhtar S, Yusoff R, Ahmad A. KEY ELEMENTS OF MARKET ORIENTATION ON MALAYSIAN SMEs PERFORMANCE. International Journal of Business and Society. 2014;15(49).

[8] Musa H, Chinniah M. Malaysian SMEs Development: Future and Challenges on Going Green. Procedia Soc Behav Sci. 2016 Jun;224:254–62.

[9] Chelliah S, Sulaiman M, Mohd Yusoff Y. Internationalization and Performance: Small and Medium Enterprises (SMEs) in Malaysia. International Journal of Business and Management. 2010 May 18;5(6).

[10] Rachagan S, Satkunasingam E. Improving corporate governance of SMEs in emerging economies: a Malaysian experience. Journal of Enterprise Information Management. 2009 Jul 24;22(4):468–84.

[11] Wang J, Neil M, Fenton N. A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. Comput Secur. 2020 Feb;89:101659.

[12] Rahman MH, Hamedani EY, Son YJ, Shafae M. Taxonomy-Driven Graph-Theoretic Framework for Manufacturing Cybersecurity Risk Modeling and Assessment. J Comput Inf Sci Eng. 2024 Jul 1;24(7).

[13] Rea-Guaman AM, San Feliu T, Calvo-Manzano JA, Sanchez-Garcia ID. Comparative Study of Cybersecurity Capability Maturity Models. In 2017. p. 100–13.

[14] Perozzo H, Zaghloul F, Ravarini A. CyberSecurity Readiness: A Model for SMEs based on the Socio-Technical Perspective. Complex Systems Informatics and Modeling Quarterly. 2022 Dec 30;(33):53–66.

[15] Ganin AA, Quach P, Panwar M, Collier ZA, Keisler JM, Marchese D, et al. Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. Risk Analysis. 2020 Jan 5;40(1):183–99.

[16] Armenia S, Angelini M, Nonino F, Palombi G, Schlitzer MF. A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decis Support Syst. 2021 Aug;147:113580.

[17] Rea-Guaman AM, Mejía J, San Feliu T, Calvo-Manzano JA. AVARCIBER: a framework for assessing cybersecurity risks. Cluster Comput. 2020 Sep 1;23(3):1827–43.

[18] Kitsios F, Chatzidimitriou E, Kamariotou M. The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. Sustainability (Switzerland). 2023 Apr 1;15(7).

[19] Clarissa S, Wang G. Assessing Information Security Management Using ISO 27001:2013. Jurnal Indonesia Sosial Teknologi. 2023 Sep 25;4(9):1361–71.

[20] Antunes M, Maximiano M, Gomes R. A Client-Centered Information Security and Cybersecurity Auditing Framework. Applied Sciences (Switzerland). 2022 May 1;12(9).

[21] Prameet P. Roy. A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. In: National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA). 2020.

[22] National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. 2024 Feb.

[23] National Institute of Standards and Technology. NIST Cybersecurity Framework 2.0: 2024 Feb. A. National Institute of Standards and Technology.

[24] Boletsis C, Halvorsrud R, Pickering J, Phillips S, Surridge M. Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment. In: Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications. SCITEPRESS - Science and Technology Publications; 2021. p. 266–74.

[25] Malatji M, Von Solms S, Marnewick A. Socio-technical systems cybersecurity framework. Information & Computer Security. 2019 Jun 12;27(2):233–72.

[26] Neri M, Niccolini F, Martino L. Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. Information & Computer Security. 2024 Jan 22;32(1):38–52.

[27] Van Haastrecht M, Yigit Ozkan B, Brinkhuis M, Spruit M. Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics. Applied Sciences. 2021 Jul 27;11(15):6909.

[28] Yigit Ozkan B, Spruit M. Adaptable Security Maturity Assessment and Standardization for Digital SMEs. Journal of Computer Information Systems. 2023 Jul 4;63(4):965–87.

[29] Yigit Ozkan, Bilge. Cybersecurity Maturity Assessment and Standardisation. Utrecht University; 2022.

[30] No WG, Vasarhelyi MA. Cybersecurity and Continuous Assurance. Journal of Emerging Technologies in Accounting. 2017 Mar 1;14(1):1–12.

[31] Gourisetti S, Mylrea M, Patangia H. Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. Future Generation Computer Systems. 2020 Apr;105:410–31.

[32] Khan M, Gide E, Chaudhry G, Hasan J. A Cybersecurity Evaluation Model (CSEM) for Indian SMEs Working in a Virtual Team Environment. In: 2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE). IEEE; 2022. p. 1–6.

[33] National Institute of Standards and Technology's. The NIST Cybersecurity Framework. In 2021. p. 171–92.

[34] Benz M, Chatterjee D. Calculated risk? A cybersecurity evaluation tool for SMEs. Bus Horiz. 2020 Jul;63(4):531–40.

[35] Dasso A, Funes A, Montejano G, Riesco D, Uzal R, Debnath N. Model-Based Evaluation of Cybersecurity Implementations. In 2016. p. 303–13.

[36] Sabillon R. The CyberSecurity Audit Model (CSAM). In 2021. p. 149–232.