Available online at https:
https://journal.uitm.edu.my/ojs/index.php/JIKM

e-ISSN: 2289-5337

Journal of Information and Knowledge Management (2026) Vol.16, No. 1

Journal of Information and Knowledge Management

Developing an Agile, Analytics-Based Information Security Maturity Framework for Malaysian SMEs: A Systematic Literature Review

Siti Zaleha Abd Goni[1*], Qamarul Nazrin Harun[2]

[1]Forest Research Institute Malaysia, 52109 Kepong, Selangor Darul Ehsan, Malaysia
[2]Faculty of Information Science, Universiti Teknologi MARA, UiTM Selangor Branch, Puncak Perdana Campus, 40150 Shah Alam, Selangor, Malaysia

Corresponding Authors' Email Address: sitizaleha.ag@gmail.com

ARTICLE INFO

Article history:
Received: 26 August 2025
Revised: 29 September 2025
Accepted: 8 January 2026
Online first
Published: 10 April 2026

Keywords:
Agile
Information security
Security maturity
Malaysian SMEs
Analytics

https://doi.org/10.24191/xjsx9r29

ABSTRACT

In the age of technology, information security has become a critical component for small and medium enterprises (SMEs), which remain highly vulnerable to cyber risks. However, most Information Security Maturity Models (ISMMs) provide limited applicability to the SME context, particularly in Malaysia, due to resource constraints, complex systems, and organizational resistance to new methodologies. This study addresses this gap by conducting a narrative review that synthesizes 30 scholarly articles published between 2022 and 2025 across leading databases. The objectives of this study are to (i) classify existing ISMM models that are relevant to SMEs, (ii) assess the extent to which these models are suitable and easy to implement by SMEs, and (iii) explore the integration of agile development approaches and analytical technologies into security maturity models. The findings reveal the need for lighter and more flexible ISMM models that enable automated digital self-assessment. Accordingly, this article proposes a conceptual three-dimensional framework that integrates agility, SME suitability, and analytic functionalities as the foundation for a contextualized ISMM for SMEs in Malaysia.

INTRODUCTION

In the age of Industrial Revolution 4.0 and the global movement towards digitalization, the need for organizational information security, particularly for small and medium enterprises

(SMEs), has become a core element in the struggle for survival and competitiveness. In Malaysia, SMEs make more than 97% of all business units, so they are a vital strength of the economy of the nation (SME Corporation Malaysia, 2022).

SMEs play an important role in the Malaysian economy, contributing to economic growth, employment opportunities, and innovation (SME Corporation Malaysia, 2022). However, size and limited resource capabilities make SMEs more vulnerable to cyber security threats (Mihelič et al., 2023). Most SMEs do not have sufficient resources to invest in an effective cyber security infrastructure, making them an accessible target to exploit (Lange & Kunz, 2024). Furthermore, the lack of awareness and training on cyber security among employees also makes SMEs more vulnerable to cyber-attacks (Sharma et al., 2022). The latest statistics refer to the Cyber999 Incident Response Center report, Q4 2024 showing that 71% of SMEs in Malaysia experienced internet fraud incidents, followed by data breach at 10% and intrusion attempts at 6% (CyberSecurity Malaysia, 2025). Due to their small size, most SMEs suffer significant losses, both financially and reputationally, after facing a cyber-attack (Ozkan & Spruit, 2022). These weaknesses show the need for SMEs to take proactive steps to improve their cyber security to ensure business survival and growth. Figure 1 is the percentage of incidents reported by categories in Q4 2024 (CyberSecurity Malaysia, 2024).

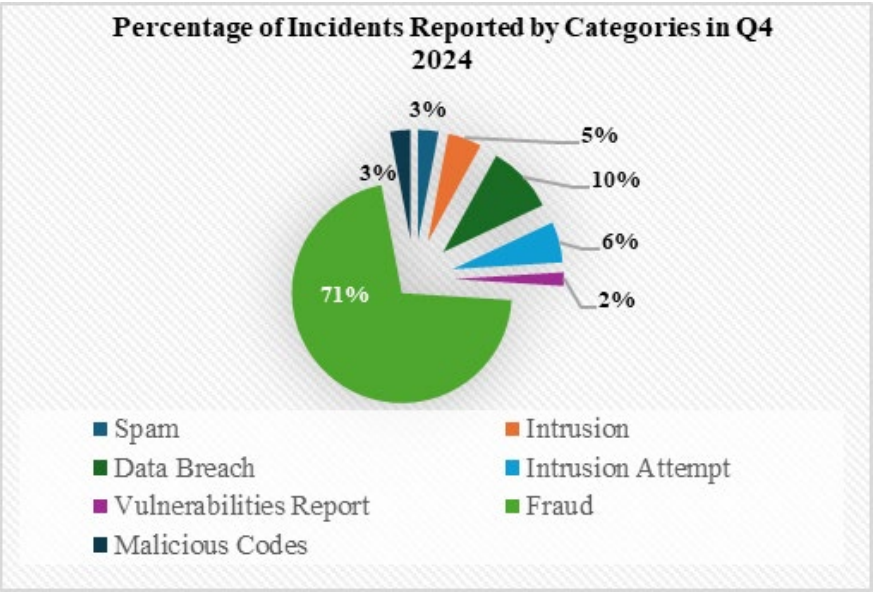

Figure 1: Percentage of Incidents Reported by Categories in Q4 2024 (CyberSecurity Malaysia, 2024)

Nevertheless, as per the study conducted by the Mihelič et al. (2023), has been observed that SMEs encounter serious difficulties in handling cyber security risk management issues because of limited resources, skill gaps, and a lack of comprehension of the digital security needs. The objectives of this study are to classify existing ISMM models that are relevant to SMEs, assess the extent to which these models are suitable and easy to implement by SMEs, and explore the

integration of agile development approaches and analytical technologies in security maturity models.

Concurrently, new approaches to software development, particularly agile, are increasingly in use, especially due to the presence of technology and innovative organizations (Sarkar et al., 2024). The implementation of agile increases flexibility, promotes continuous feedback, and enables quick execution. But, when this approach is mixed with information security needs, it presents new issues as security processes are often at odds with agile principles. These processes are typically slow, require extensive documentation, and are not adaptable. Several research works have tried to solve the problem with novel methods, like the adaptive ASMAS model for SMEs (Ozkan & Spruit, 2022) and the hybrid model that integrates elements of Scrum and maturity evaluation (Kadenic et al., 2023). In fact, the incorporation of analytics into security models facilitates the possibility for active monitoring, real-time risk assessment, and improvement through machine learning empowered decision-making (Brezavšček & Baggia, 2025).

However, based on a review of 30 articles, it was found that most existing models:

1. Not suitable for SMEs
2. Too heavy and difficult to implement
3. Does not support integration with agile methods
4. Does not fully leverage analytics technology

Table 1: Key Challenges of Existing Security Maturity Models

Challenges	Authors	Impact on SMEs
Models are too complex and inflexible	Brezavšček & Baggia, 2025; Liyanage et al., 2024; Sharma et al., 2022; Vasylieva et al., 2023	Difficult to implement by SMEs with limited resources
No support for agile approaches	Ardo et al., 2022; Lange & Kunz, 2024; Tøndel et al., 2022	Fail to integrate security into development
Not suitable for SME context	Mihelič et al., 2023; Ozkan & Spruit, 2022; Re et al., 2023a; Selva-Mora & Quesada-López, 2024; Surya et al., 2024	Not practical or too costly
No analytical/data-driven elements	Brezavšček & Baggia, 2025; Ozkan & Spruit, 2022; Van De Poll & Duricic, 2024	Difficult to assess performance and make improvements

In this regard, this article aims to conduct a comprehensive review of existing information security maturity models with a focus on:

1. Agile integration – i.e. how the model supports agile development
2. Compatibility with Malaysian SMEs – i.e. the level of flexibility and entrepreneurship
3. Analytical elements – i.e. the level of automation, data visibility and assessment adaptability

LITERATURE REVIEW

Relevant studies highlight that the incorporation of information security within agile software development processes continues to have a number of practical limitations, particularly among some small and SMEs. The literature to be discussed was organized and developed under three primary headings: agile and security approaches, information security maturity models (ISMM), and modifications for SMEs.

Agile and Information Security

The iterative nature of Agile software development fosters flexibility, collaboration, and continuous implementation. However, these practices often clash with rigid standards of information security, especially in compliance, documentation, and control access. Researches done by the authors Lange & Kunz, 2024 and Sharma et al. (2022) indicate that most traditional secure development lifecycle (SDL) models still remain incompatible with agile processes, which results in the integration of security being done at later stages of the development cycle.

The authors Mihelič et al. (2023) propose a lighter set of security components suitable for SMEs, but argue that there exists considerable conflict between the demands of agility and compliance to security. On addressing this concern, models like CAESAR8 (Loft et al., 2022) have developed an enterprise architecture (EA) model that attempts to blend agility with security control, while the Scrum maturity model (Kadenic et al., 2023) underlines the role, values, and actions of teams such as security backlogs and security sprints as crucial for fostering integrated security within the agile environment.

Information Security Maturity Model (ISMM)

The ability of an organization to manage security risks has led to the development of several information security maturity models, such as Building Security In Maturity Model (BSIMM), Open Web Application Security Project (OWASP), Software Assurance Maturity Model (SAMM), and Cybersecurity Maturity Model Certification (CMMC). Most of these models, however, seem to be overly formal and complicated, which makes it more difficult to implement in smaller scale organizations such as SMEs. The authors Brezavšček & Baggia (2025), Liyanage et al. (2024) and Vasylieva et al. (2023) have evaluated the inflexibility of these models and the need for them to be more responsive and adaptive to modern and digital realities.

Furthermore, to address the shortcomings of the existing models, Ozkan & Spruit (2022), introduced the Adaptable Security Maturity Assessment and Standardization (ASMAS) model, which is modular and less heavy on security measures, making it more appropriate for SMEs. The model allows changes to be made depending on the maturity level and capability of the organization, thus lessening the implementation burden. In the financial context, the Surya et al. (2024) put forth an aimed incremental plan for applying ISO 27001:2022, which is meant for fostering the security maturity of small and newer financial institutions.

The two models illustrate that a modular model based on capabilities is more useful than the all-inclusive model employed by many large businesses.

Focus on SMEs and Contextual Needs

The aforementioned SMEs have distinctive drawbacks such as inadequately trained personnel, insufficient technology, and a low information security appreciative attitude. Ali & Wasim (2022), Lange & Kunz, 2024 and Mihelič et al. (2023) assert that more than half of SMEs do not adopt agile or security measures because there is no enabling conceptual framework to guide them. Within the Malaysian context, studies by Surya et al. (2024) recommend that these small firms be given some tailored operational reality based stage criteria for these phases. According to Edú et al. (2023), Omowole et al. (2024), Re et al. (2023) and Selva-Mora & Quesada-López (2024), similarly proclaim the importance of operational self-evaluation and automation in repositioning the security function to facilitate the conduct of business.

Table 2: Highlights of Previous Studies Based on Focus

Focus	Authors	Main Highlights
Agile and Security	Ardo et al., 2022; Kadenic et al., 2023; Lange & Kunz, 2024; Loft et al., 2022; Mihelič et al., 2023; Nägele et al., 2024; Sallam et al., 2023; Sharma et al., 2022; Tøndel et al., 2022; Vasylieva et al., 2023	The conflict between agility and security
Maturity Model (ISMM)	Brasoveanu et al., 2022; Brezavšček & Baggia, 2025; Corona et al., 2022; Handri et al., 2024; Lange & Kunz, 2024; Liyanage et al., 2024; Ozkan & Spruit, 2022; Van De Poll & Duricic, 2024; Vasylieva et al., 2023	The unsuitability of large models for SMEs
Focus on SMEs	Ali & Wasim, 2022; Edú et al., 2023; Mihelič et al., 2023; Nägele et al., 2023; Omowole et al., 2024; Ozkan & Spruit, 2022; Re et al., 2023; Selva-Mora & Quesada-López, 2024; Surya et al., 2024	The need for flexibility, cost efficiency, and locality
Analytics/Data -Driven	Arnarson et al., 2022; Brezavšček & Baggia, 2025; Corona et al., 2022; Lange & Kunz, 2024; Liyanage et al., 2024; Ozkan & Spruit, 2022	Dynamic assessment and progress visualization

In light of agile, analytics-based, and SME-friendly considerations applicable to the Malaysian context, this literature review has showcased a variety of models and approaches that, as of yet, have been able to satisfy all requirements. Hence, there is a significant gap in existing structural literature that must be overcome by establishing an agile, context-sensitive, and analytics-friendly framework.

METHODOLOGY

This study uses a narrative review approach that incorporates aspects of systematic (Braun & Clarke, 2022) to evaluate and integrate 30 scholarly articles on information security, agile security development, security maturity, and SME specific focus analysis. These reviewed articles are from recognized journals and were published from 2022 to 2025. A systematic literature review has been undertaken for both scholastic and non-scholastic sources, such as peer-reviewed journals and conference papers, to incorporate theoretical and practical views for a comprehensive analysis. This systematic review approach was chosen to cover the topic as comprehensively as

possible. Although the number of selected articles is limited to 30, it encompasses a wide range of important perspectives from the recent period and is therefore adequate for a complete analysis.

The main source for obtaining information and data related to this research is research literature collected from various databases, including the Google Scholar database, ACM digital library, Emerald Insight, Science Direct, Taylor & Francis, and IEEE Xplore. In addition, Google search engines were utilized to gather research-related information.

The selection of the articles was done on the basis of three core principles:

1. Examining an information security framework or model.
2. Incorporating agile development concepts or practices.
3. Restricting the scope to SMEs.

Exclusion criteria included non-peer-reviewed sources such as blogs or news reports, studies published before 2022, and articles that did not directly address ISMM, agile development, or SME-specific contexts.The articles were analyzed and organized in relation to the primary themes of the study to achieve its primary aims.

Table 3: Classification of Articles by Research Themes

Research Theme	Number of Articles	Authors
Agile and Information Security	10	Ardo et al., 2022; Kadenic et al., 2023; Lange & Kunz, 2024; Loft et al., 2022; Mihelič et al., 2023; Nägele et al., 2024; Sallam et al., 2023; Sharma et al., 2022; Tøndel et al., 2022; Vasylieva et al., 2023
Security Maturity Model (ISMM)	9	Brasoveanu et al., 2022; Brezavšček & Baggia, 2025; Corona et al., 2022; Handri et al., 2024; Lange & Kunz, 2024; Liyanage et al., 2024; Ozkan & Spruit, 2022; Van De Poll & Duricic, 2024; Vasylieva et al., 2023
Focus on SME	9	Ali & Wasim, 2022; Edú et al., 2023; Mihelič et al., 2023; Nägele et al., 2023; Omowole et al., 2024; Ozkan & Spruit, 2022; Re et al., 2023; Selva-Mora & Quesada-López, 2024; Surya et al., 2024
Integration of Analytical/Data-Driven Elements	6	Arnarson et al., 2022; Brezavšček & Baggia, 2025; Corona et al., 2022; Lange & Kunz, 2024; Ozkan & Spruit, 2022; Surya et al., 2024

This thematic analysis seeks to systematically compare the articles based on their objectives, employed methods, primary findings, and relevance to the context of SMEs in Malaysia. It should be pointed out that an article may fall under several themes, so the total count of articles under all themes is greater than 30. This thematic design permits a structured analysis of comparative study objectives, methodologies, principal contributions, and the relevance of each study within the context of SMEs in Malaysia. Such analysis will understand the extent to which the existing frameworks are suitable and the rationale that will be provided for the need for the development of a new conceptual framework that is more flexible and functional will be underscored.

ANALYSIS AND FINDING

The analysis of the 30 studies selected reveals that there are numerous methods suggested for evaluating and enhancing information security maturity in an organization, most of which are not ready for implementation in the context of Malaysian SMEs. This research synthesizes the findings using three dimensions: alignment with agile methodology, targeting SMEs, and application of analytics. Considering agile practices, other authors within Sharma et al. (2022), CAESAR8 by Loft et al. (2022) and Mihelič et al. (2023), pointed out the necessity to profound iterative security integration into software engineering processes. Meanwhile, most conventional frameworks like Microsoft SDL or BSIMM (Lange & Kunz, 2024; Liyanage et al., 2024) seem to remain rigid and not flexible enough to accommodate scrum or DevOps procedures.

Within the context of SME, there provisionally lies some limited range of research that concentrates on the specific problems and requirements of SMEs. These are ASMAS (Ozkan & Spruit, 2022), a model for BPRDCo using ISO 27001:2022 (Surya et al., 2024), and a lightweight assessment model for agile manufacturing (Ali & Wasim, 2022). The authors of Ali & Wasim (2022) and Ozkan & Spruit (2022) say that the degree of success greatly relies on the amount of effort put in relative to the expectations from the small organization.

The research gaps are and remain substantial in the dimension of analytical integration. While some self-evaluation or automated metric examples are presented by Brezavšček & Baggia (2025), Corona et al. (2022) and Ozkan & Spruit (2022), the application of analytics as one of the primary constituents in measuring maturity is still not common. There are models like in Brezavšček & Baggia (2025) that propose metric-based visualization as a major feature enhancement, but there is no single model which fully incorporates analytics into the agile paradigm.

Table 4: Article Evaluation Based on Three Main Dimensions

Authors	Agile	SME Focus	Analytics	Notes
Ali & Wasim, 2022	x	/	x	Agile manufacturing impact assessment
Ardo et al., 2022	/	x	x	Agile process integration model
Arnarson et al., 2022	/	x	x	Maturity technologies in agile manufacturing
Brasoveanu et al., 2022	x	x	x	Security maturity self-assessment framework
Braun & Clarke, 2022	x	x	x	Guide to thematic analysis methodology used in review
Brezavšček & Baggia, 2025	x	x	/	Touching on metrics usage and trends
Corona et al., 2022	/	x	x	Agile method evaluation proposal
Edú et al., 2023	x	/	x	Cybersecurity framework for SMEs in Peru
Handri et al., 2024	/	x	x	Agile cybersecurity using Q methodology
Kadenic et al., 2023	/	x	x	Scrum maturity with team focus
Lange & Kunz, 2024	x	x	/	Critical review of SDL and SMM
Lee et al., 2025	x	x	x	Adaptation of CMMI in developing countries
Liyanage et al., 2024	x	x	x	Gap analysis of CCMM models
Loft et al., 2022	/	x	x	EA approach to agile security

Authors	Agile	SME Focus	Analytics	Notes
Mihelič et al., 2023	/	/	x	Suitable for SMEs, lacks analytical elements
Nägele et al., 2023	/	x	x	Compliance maturity & governance review
Nägele et al., 2024	/	x	x	Security governance for agile enterprise
Omowole et al., 2024	x	/	/	Agile practices for economic resilience in SMEs
Ozkan & Spruit, 2022	/	/	/	Best adaptive model to date
Re et al., 2023	x	/	/	SME digitalization through maturity models
Re et al., 2023	x	x	x	SME digital maturity mapping
Sallam et al., 2023	/	x	/	Agile maturity linked to transformation
Sarkar et al., 2024	/	x	x	Trends in agile software development
Selva-Mora & Quesada-López, 2024	/	/	/	Security practices in agile development
Sharma et al., 2022	/	x	x	Early study of agile and security integration
Surya et al., 2024	x	/	x	ISO 27001 case study for small banks
Tøndel et al., 2022	/	/	/	Security prioritization in agile projects
Van De Poll & Duricic, 2024	/	/	/	ISMM redesign for agile transformation
Vasylieva et al., 2023	x	x	/	Evaluation of agile maturity models
Wilson & McDonald, 2025	x	x	x	Cybersecurity needs of UK SMEs

This analysis confirms that no single article integrates agile methodology and analytics with SME requirements into an information security maturity model. This further supports the need for a new framework that is contextually and structurally flexible to cater to SMEs in Malaysia.

The outcomes of the analysis conducted on 30 articles reveals that most available information security maturity models are still inadequate for small organizations like SMEs, particularly in Malaysia. These outcomes are categorized into three principal areas.

Agile and Security Integration Constraints

Although certain models endorse agile practices, few incorporate security throughout the agile workflow. The authors' studies Mihelič et al., 2023; Sharma et al. (2022) indicate that most organizations find it difficult to encapsulate security activities within the operational sprints and backlogs. CAESAR8 by Loft et al. (2022) tries to address this problem by restructuring an organization's architecture to be more agile compliant.

Models Not Adapted for SMEs

Ali & Wasim (2022), Ozkan & Spruit (2022) and Surya et al. (2024) claim that current frameworks like BSIMM and ISO 27001 are too sophisticated and burdensome for SMEs. Models used by SMEs need to be simple, flexible, and resource efficient. ASMAS (Ozkan & Spruit, 2022) and the ISMS implementation roadmap model (Surya et al., 2024) proves that a combination of modular and phased strategy is efficient.

Use of Analytics Still Limited

While the authors Brezavšček & Baggia (2025), Lange & Kunz (2024) and Ozkan & Spruit (2022) indicated increased interest in using data and automation for maturity assessments, most models still lack automation as a principal feature. This indicates a noteworthy chance to develop new frameworks that depend on data and real-time graphical representation.

Table 5: Summary of Key Findings Based on Study Dimensions

Dimension	Key Findings	Authors
Agile	Constraints of security integration in scrum and DevOps processes	Ardo et al., 2022; Loft et al., 2022; Mihelič et al., 2023; Sharma et al., 2022; Tøndel et al., 2022
SME suitability	Existing models are too complex for SMEs	Ali & Wasim, 2022; Ozkan & Spruit, 2022; Selva-Mora & Quesada-López, 2024; Surya et al., 2024
Analytical Elements	Use of metrics and visual monitoring is still rudimentary	Brezavšček & Baggia, 2025b; Corona et al., 2022; Lange & Kunz, 2024; Liyanage et al., 2024; Ozkan & Spruit, 2022
Agile	Constraints of security integration in scrum and DevOps processes	Ardo et al., 2022; Loft et al., 2022; Mihelič et al., 2023; Sharma et al., 2022; Tøndel et al., 2022

The findings of this study affirm that an agile, lightweight, and analytics-based ISMM framework has not been fully formed, demonstrating the necessity to create a model tailored to SMEs in Malaysia.

DISCUSSIONS AND CONCLUSION

An evaluation of 30 articles reveals that current methods for evaluating security information fail to meet the requirements of SMEs operating in an agile environment in Malaysia. The discussed issues are: barriers to agile integration, model non-compliance with SMEs, and absence of analytical capabilities.

Models already in existence, like Microsoft's SDL and OWASP SAMM (Lange & Kunz, 2024; Liyanage et al., 2024; Sharma et al., 2022), are much more appropriate for large companies that already have detailed software development and security processes in place. In contrast, ASMAS (Ozkan & Spruit, 2022) and the BPRDCo model (Surya et al., 2024) are more accommodating to SMEs as they provide custom modular designs, agile structures, and implementation plans that match the restricted human and technological resources available.

Pertaining to agile approaches, the authors' studies Mihelič et al. (2023) and Ozkan & Spruit (2022), reveal that the efficacy of Scrum and other agile frameworks stems from the level of team maturity, security knowledge, and incorporation of security integrations into agile-specified roles and activities. This underscores the critical gap for an ISMM model that works within the bounds of agile development's iterative and collaborative nature.

In addition, the employment of evaluation analytics as proposed by the authors of Brezavšček & Baggia (2025) and Ozkan & Spruit (2022) can improve the capability of SMEs to assess security evolution in real time, construct assessments based on facts, and automatically detect crucial discrepancies.

Table 6: Matching Results According to Study Objectives

Objectives	Key Findings	Authors
Objective 1: Agile + ISMM	Challenges of security integration in agile processes	Kadenic et al., 2023; Lange & Kunz, 2024; Loft et al., 2022; Mihelič et al., 2023; Sharma et al., 2022; Tøndel et al., 2022
Objective 2: SME-Friendly	Existing models are too heavy, need for modular & lightweight models	Ali & Wasim, 2022; Ozkan & Spruit, 2022; Re et al., 2023; Selva-Mora & Quesada-López, 2024; Surya et al., 2024
Objective 3: Analytics-based ISMM	Visual and automated assessments are still underused	Brezavšček & Baggia, 2025; Corona et al., 2022; Lange & Kunz, 2024; Liyanage et al., 2024; Ozkan & Spruit, 2022
Objective 1: Agile + ISMM	Challenges of security integration in agile processes	Kadenic et al., 2023; Lange & Kunz, 2024; Loft et al., 2022; Mihelič et al., 2023; Sharma et al., 2022; Tøndel et al., 2022

In the SMEs context, these results reinforce the justification of the need to develop an information security maturity framework that is agile, analytically driven and appropriate to the actual context of SMEs in Malaysia.

Conceptual Framework

Based on the literature analysis and study findings, a conceptual framework is proposed to develop an agile and analytics-driven information security maturity framework, specifically to support the needs of SMEs in Malaysia.

The framework is composed of three main components:

1. Agile Dimension – Adapts Scrum roles, such as Product Owner, Scrum Master and Developer (Kadenic et al., 2023), as well as repetitive and iterative activities in security (Loft et al., 2022; Mihelič et al., 2023; Sharma et al., 2022).
2. SME-aware Dimension – Provides a modular, lightweight and adaptable approach with limited resources (Ali & Wasim, 2022; Ozkan & Spruit, 2022; Surya et al., 2024).
3. Analytical Dimension – Integrates real-time progress visualization, maturity metrics and digital self-assessment (Brezavšček & Baggia, 2025; Corona et al., 2022; Lange & Kunz, 2024; Ozkan & Spruit, 2022).

Table 7: Recommended Components of The ISMM Agile-Analytics Conceptual Framework for SMEs

Components	**Key Features**	**Authors**
Agile	Roles, security backlog, dedicated sprints	Ardo et al., 2022; Kadenic et al., 2023; Loft et al., 2022; Mihelič et al., 2023; Sharma et al., 2022
SME-aware	Modular, lightweight, phased roadmap	Ali & Wasim, 2022; Ozkan & Spruit, 2022; Re et al., 2023; Selva-Mora & Quesada-López, 2024; Surya et al., 2024
Analytics-based	Visual assessment, automation, data monitoring	Brezavšček & Baggia, 2025; Corona et al., 2022; Lange & Kunz, 2024; Liyanage et al., 2024; Ozkan & Spruit, 2022

This model can serve as the foundation for building a realistic, adaptable, and locally relevant security maturity assessment model for small and medium enterprises (SMEs), thus improving their cyber resilience in a digitally driven environment.

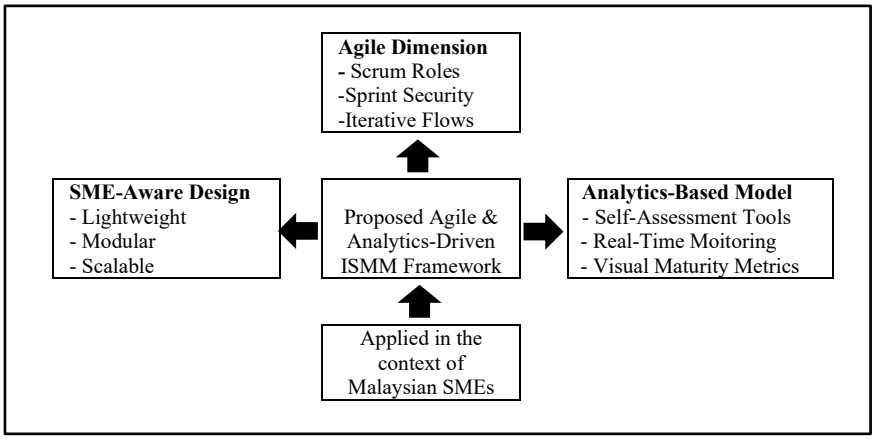

Figure 2: The ISMM Agile-Analytics Conceptual Framework for SMEs

Models such as ASMAS (Ozkan & Spruit, 2022), CAESAR8 (Loft et al., 2022), and the mature scrum approach (Kadenic et al., 2023) provide a solid foundation, but need to be adapted to the actual operating context of SMEs in Malaysia. In addition, analytical elements such as digital self-assessment and visual monitoring have not yet been fully integrated into existing models (Brezavšček & Baggia, 2025; Lange & Kunz, 2024; Liyanage et al., 2024).

Accordingly, a conceptual framework was proposed that combines agile dimensions, SME-friendly design, and analytics approaches to form a more practical and contextual ISMM model. The objectives of this study include theory, practice and further research contribution. As for theory, this research identifies relevant gaps within the existing ISMM model. It also provides an ISMM framework that addresses the practical needs of SMEs in Malaysia for the purpose of practice. Relating to research, it describes the necessity of more comprehensive validation through case studies for local SMEs.

Framework provides directions for further research which includes building a prototype evaluation system and conducting case studies with local SMEs to test applicability and effectiveness in practice.

ACKNOWLEDGMENT

Authors acknowledge the Ministry of Higher Education (MOHE) for funding under the Fundamental Research Grant Scheme (FRGS/1/2024/SS02/UITM/02/1).

REFERENCES

Ali, A., & Wasim, A. (2022). Innovative framework for assessing the impact of agile manufacturing in small and medium enterprises (SMEs). *Sustainability*, *14*(18), 11503. https://doi.org/10.3390/su141811503

Ardo, A., Bass, J., & Gaber, T. (2022). Towards secure agile software development process: A practice-based model. *2022 48th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, 149–156. https://doi.org/10.1109/SEAA56994.2022.00031

Arnarson, H., Kanafi, F. S., Kaarlela, T., Seldeslachts, U., & Pieters, R. (2022). Evaluation of cyber security in agile manufacturing: Maturity of Technologies and Applications. *2022 IEEE/SICE International Symposium on System Integration (SII)*, 784–789. https://doi.org/10.1109/SII52469.2022.9708888

Brasoveanu, R., Karabulut, Y., & Pashchenko, I. (2022, August 23). Security maturity self-assessment framework for software development lifecycle. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3538969.3543806

Braun, V., & Clarke, V. (2022). *Thematic analysis: A practical guide*. SAGE Publications.

Brezavšček, A., & Baggia, A. (2025). Recent trends in information and cyber security maturity assessment: A systematic literature review. *Systems*, *13*(1), 52. https://doi.org/10.3390/systems13010052

Corona, B., Muñoz, M., & Mejía, J. (2022). A proposal for assessing and evolving an agile software development method. *2022 10th International Conference in Software Engineering Research and Innovation (CONISOFT)*, 11–18. https://doi.org/10.1109/CONISOFT55708.2022.00013

CyberSecurity Malaysia. (2025). *SR-029.022025: MyCERT Report - Cyber Incident Quarterly Summary Report - Q4 2024*. https://www.mycert.org.my/portal/advisory?id=SR-029.022025

Edú, M., Alexis, G., & Lenis, W. (2023). Cybersecurity framework for SMEs in Peru based on ISO/IEC 27001 and CSF NIST controls. *2023 18th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–7. https://doi.org/10.23919/CISTI58278.2023.10211874

Handri, E., Sensuse, D., & Tarigan, A. (2024). Developing an agile cybersecurity framework with organizational culture approach using Q methodology. *IEEE Access*, *12*, 108835–108850. https://doi.org/10.1109/ACCESS.2024.3432160

Kadenic, M., Koumaditis, K., & Junker-Jensen, L. (2023). Mastering scrum with a focus on team maturity and key components of scrum. *Information and Software Technology*, *153*, 107079. https://doi.org/10.1016/j.infsof.2022.107079

Lange, F., & Kunz, I. (2024). Evolution of secure development lifecycles and maturity models in the context of hosted solutions. *Journal of Software: Evolution and Process*, *36*(12). https://doi.org/10.1002/smr.2711

Lee, G. S., Kim, S. H., Lee, I. Y., Brown, S., & Carbajal, Y. A. (2025). Adapting cybersecurity maturity models for resource-constrained settings: A case study of Peru. *Electronic Journal of Information Systems in Developing Countries*, *91*(1). https://doi.org/10.1002/isd2.12350

Liyanage, L., Arachchilage, N., & Russello, G. (2024). *SoK: Identifying Limitations and Bridging Gaps of Cybersecurity Capability Maturity Models (CCMMs)*. http://arxiv.org/abs/2408.16140

Loft, P., He, Y., Yevseyeva, I., & Wagner, I. (2022). CAESAR8: An agile enterprise architecture approach to managing information security risks. *Computers & Security*, *122*, 102877. https://doi.org/10.1016/j.cose.2022.102877

Mihelič, A., Vrhovec, S., & Hovelja, T. (2023). Agile development of secure software for small and medium-sized enterprises. *Sustainability*, *15*(1), 801. https://doi.org/10.3390/su15010801

Nägele, S., Schenk, N., Fechtner, N., & Matthes, F. (2024). Balancing autonomy and control: An adaptive approach for security governance in large-scale agile development. *Proceedings of the 26th International Conference on Enterprise Information Systems*, 17–28. https://doi.org/10.5220/0012605000003690

Nägele, S., Schenk, N., & Matthes, F. (2023). The Current state of security governance and compliance in large-scale agile development: A systematic literature review and interview study. *2023 IEEE 25th Conference on Business Informatics (CBI)*, 1–10. https://doi.org/10.1109/CBI58679.2023.10187439

Omowole, B., Olufemi-Phillips, A., Ofodile, O., Eyo-Udo, N., & Ewim, S. (2024). Conceptualizing agile business practices for enhancing SME resilience to economic shocks. *International Journal of Scholarly Research and Reviews*, *5*(2), 070–088. https://doi.org/10.56781/ijsrr.2024.5.2.0049

Ozkan, B., & Spruit, M. (2022). Adaptable security maturity assessment and standardization for digital SMEs. *Journal of Computer Information Systems*, *63*(4), 965–987. https://doi.org/10.1080/08874417.2022.2119442

Re, N., Ghezzi, A., Balocco, R., & Rangone, A. (2023). Supporting the digitalization of SMEs through maturity models. *European Conference on Innovation and Entrepreneurship*, *18*(2), 763–771. https://doi.org/10.34190/ecie.18.2.1822

Sallam, S., Fouad, M., & Hemeida, F. (2023). Relationship between agile maturity and digital transformation Success. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *33*(3), 154–168. https://doi.org/10.37934/araset.33.3.154168

Sarkar, T., Moharana, B., Rakhra, M., & Cheema, G. (2024). Comparative analysis of empirical research on agile software development approaches. *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2024*. https://doi.org/10.1109/ICRITO61523.2024.10522134

Selva-Mora, A., & Quesada-López, C. (2024). Security practices in agile software development: A mapping study. *Proceedings of the 7th ACM/IEEE International Workshop on Software-Intensive Business*, 56–63. https://doi.org/10.1145/3643690.3648241

Sharma, S., Singh, G., Jones, P., Kraus, S., & Dwivedi, Y. (2022). Understanding agile innovation management adoption for SMEs. *IEEE Transactions on Engineering Management*, *69*(6), 3546–3557. https://doi.org/10.1109/TEM.2022.3148341

SME Corporation Malaysia. (2022). *MSME Insights: MSMEs towards sustainable recovery* (2021 edition).

Surya, I. C., Mulyana, R., & Nugraha, R. A. (2024). BPRDCo SME digital transformation by designing information security using ISO 27001:2022. *Jurnal JTIK (Jurnal Teknologi Informasi Dan Komunikasi)*, *8*(4), 1242–1253. https://doi.org/10.35870/jtik.v8i4.3148

Tøndel, I., Cruzes, D., Jaatun, M., & Sindre, G. (2022). Influencing the security prioritisation of an agile software development project. *Computers & Security*, *118*, 102744. https://doi.org/10.1016/j.cose.2022.102744

Van De Poll, J., & Duricic, J. (2024). Redesigning maturity models when rolling out agile transformations. *European Journal of Business and Management Research*, *9*(1), 15–20. https://doi.org/10.24018/ejbmr.2024.9.1.2039

Vasylieva, K., Kuhrmann, M., Xavier, M., & Klünder, J. (2023). How agile are you? Discussing maturity levels of agile maturity models. *2023 49th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, 270–277. https://doi.org/10.1109/SEAA60479.2023.00049

Wilson, M., & McDonald, S. (2025). One size does not fit all: Exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses. *Information Security Journal*, *34*(1), 15–49. https://doi.org/10.1080/19393555.2024.2357310

Zaini, M. K., Masrek, M. N., & Abdullah Sani, M. K. J. (2020). The impact of information security management practices on organisational agility. *Information & Computer Security*, *28*(5), 681-700.