International Journal on Advanced Science Engineering Information Technology

Vol.14 (2024) No. 5
ISSN: 2088-5334

Evolution of Information Security Awareness towards Maturity: A Systematic Review

Mohd Ridzam Ahmad [a,b], Mohd Hafeez Osman [a,*], Azizol Abdullah [a], Khaironi Yatim Sharif [c]

[a] *Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Serdang, Selangor, Malaysia*
[b] *National Digital Department, Cyberjaya, Sepang, Selangor, Malaysia*
[c] *Universiti Teknologi Petronas, Seri Iskandar, Perak, Malaysia*
*Corresponding author: *hafeez@upm.edu.my*

***Abstract*— This systematic review provides an in-depth analysis of existing information security awareness (ISA) maturity models. This review synthesizes findings from 25 scholarly articles, identifying standard dimensions such as risk management, organizational culture, training programs, policy compliance, and technical measures. Despite diverse approaches, significant gaps are evident, particularly the absence of tailored models for specific organizational types like public sector entities. Additionally, the reliance on self-reported data and expert opinions in many models introduces biases, limiting their applicability. The findings underscore the need for organizations to adopt a comprehensive approach to ISA maturity, combining technical controls with behavioral assessments. This holistic view is essential for developing robust ISA maturity frameworks to address evolving cyber threats. Emphasizing compliance with established standards, such as ISO/IEC 27001, is critical to enhancing ISA across industries. Future research should focus on validating and refining ISA maturity models in diverse contexts and industries. This includes testing models in different organizational settings to ensure broader applicability and developing frameworks integrating technical and behavioral dimensions. Addressing sector-specific tailoring, integrating technical and managerial aspects, and providing rigorous empirical validation are critical for developing more effective and adaptable models. Developing ISA maturity models specifically tailored for the public sector is vital due to these organizations' unique challenges and responsibilities. Utilizing updated versions of standards like ISO 27000 series provides a robust framework for maintaining high information security awareness and preparedness standards.**

***Keywords*— Information Security Awareness (ISA); maturity model; cybersecurity frameworks; ISO/IEC 27001.**

Manuscript received 5 Jun. 2024; revised 4 Aug. 2024; accepted 11 Sep. 2024. Date of publication 31 Oct. 2024.

I. INTRODUCTION

Information security awareness (ISA) has become critical in safeguarding organizational assets against the increasing complexity and frequency of cyber threats. The importance of ISA lies in its ability to mitigate human-related risks, which are often the weakest link in an organization's security chain [1], [2], [3]. A structured approach to enhancing ISA can be achieved through the implementation of maturity models, which provide a framework for evaluating and improving security awareness levels systematically [4], [5]. This systematic literature review (SLR) aims to synthesize existing research on information security awareness maturity models, identify gaps, and propose future research directions to advance the field.

ISA is crucial for the effective management of information security within organizations. Adriko and Nurse emphasize the role of cybersecurity in the value proposition of cyber insurance for small-to-medium-sized enterprises (SMEs), highlighting the importance of awareness in enhancing security postures [6]. Rizal and Setiawan further stress that measuring security awareness is essential for improving individual behavior towards security practices, which in turn strengthens the overall security posture of an organization [7]. Similarly, Gwenhure and Rahayu [8] highlight the impact of gamification on cybersecurity awareness among non-IT professionals, demonstrating the effectiveness of innovative methods in enhancing ISA. These studies underscore the need for comprehensive models to assess and elevate security awareness across different organizational contexts.

Maturity models provide a structured pathway for organizations to advance from basic to advanced security awareness levels. According to Marican et al. [9], existing cybersecurity maturity assessment frameworks often lack a

focus on end-to-end solutions for technology startups, indicating a need for more tailored approaches. This is further supported by Ukeje et al. [10], who identify significant gaps in information security and privacy in cloud computing for government adoption, emphasizing the importance of robust frameworks that include awareness components. These insights highlight the necessity for a focused SLR that consolidates existing knowledge on ISA maturity models and identifies areas for improvement.

Despite various maturity models, a notable lack of unified frameworks specifically addressing information security awareness exists. Many models, such as the Cyber Security Maturity Assessment Framework for Technology Startups, point out the need for comprehensive frameworks but fall short of providing specific guidelines for security awareness [9]. Additionally, studies by Chaudhary et al. reveal a pressing need for research on cybersecurity awareness tailored to small and medium-sized enterprises (SMEs), which often lack the resources and expertise to prioritize security effectively [11]. These gaps indicate a significant opportunity to develop and refine maturity models that focus explicitly on enhancing ISA.

Previous research has also highlighted the challenges associated with evaluating the long-term effectiveness of ISA initiatives. For instance, Gwenhure and Rahayu [8] identified gaps in the long-term evaluation of gamified cybersecurity awareness programs, suggesting the need for ongoing assessment and adaptation of these programs to ensure sustained effectiveness. Furthermore, Ukeje et al. [10] emphasize the importance of addressing privacy concerns in cloud computing, which are often overlooked in current maturity models . These issues underline the importance of developing comprehensive ISA maturity models that incorporate long-term evaluation and address privacy concerns.

This SLR aims to fill the critical gap in the existing literature by focusing exclusively on information security awareness maturity models. While earlier studies have explored various dimensions of cybersecurity maturity, including technical and managerial aspects, this review explicitly addresses the awareness component. By consolidating and analyzing models focusing on ISA, this SLR provides a detailed understanding of how awareness is measured and enhanced within organizations. This focused approach allows for identifying best practices and developing more effective and targeted ISA programs.

Additionally, this review will highlight the differences between existing ISA maturity models and propose improvements based on identified gaps. For example, the study by Rizal and Setiawan facilitates the selection of focus areas for measuring security awareness, which can be integrated into future models to enhance their effectiveness [7]. Similarly, insights from Chaudhary et al. on the specific needs of SMEs can be used to tailor ISA maturity models to address the unique challenges faced by these organizations [11]. This SLR consolidates existing knowledge and provides actionable recommendations for advancing the field of ISA maturity models.

The objectives of this SLR are to provide a comprehensive overview of existing maturity models for information security awareness, identify common areas, dimensions, and maturity levels covered by these models, analyze the gaps and limitations present in current models, propose recommendations for improving ISA maturity models, and highlight the practical implications for organizations aiming to enhance their security awareness. By achieving these objectives, this review aims to contribute to the field of ISA by offering a detailed analysis and synthesis of existing knowledge, identifying research gaps, and proposing future directions for developing more effective ISA strategies. Based on the above objectives, we formulated three research questions:

a. What are the existing maturity models for information security awareness?
b. What are the common dimensions and levels included in these models?
c. What are the identified gaps and limitations in current ISA maturity models?

Section II outlines the methodology employed in this review, providing a comprehensive description of the procedures and techniques used to investigate the objectives. Subsequently, Sections III and IV present the findings and engage in an in-depth discussion of the obtained results. Section IV culminates the review by offering a conclusive summary of the findings, including identifying limitations encountered during the study and providing recommendations for future research endeavors.

II. Material and Method

A. Methodology

This systematic literature review (SLR) adheres to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. PRISMA, developed by [12], provides a comprehensive framework for conducting high-quality systematic reviews by emphasizing clarity in research questions, thoroughness in literature search, and rigor in quality assessment.

PRISMA was selected due to its robustness in ensuring methodological rigor and transparency. It emphasizes the importance of quality in articles chosen and encourages researchers to develop straightforward research questions. Furthermore, PRISMA promotes comprehensive and relevant literature searches, ensuring that the review covers all pertinent studies. Although PRISMA is predominantly used in medical and health-related fields, its flexibility makes it suitable for other disciplines, including information security awareness maturity models. This adaptability is supported by [7] and [8], who highlight PRISMA's suitability for diverse research contexts.

Guided by PRISMA, this review began with formulating research questions using the PICo method: ‘P’ for Problem or Population, ‘I’ for Interest, and ‘Co’ for Context. The systematic search strategy followed three phases: identification, screening, and eligibility. A quality appraisal process was conducted using criteria adapted from existing literature, ensuring the inclusion of high-quality studies. The selected articles underwent data extraction and thematic synthesis, focusing on the primary research questions. This systematic approach, as outlined by PRISMA, ensures the reliability and validity of the review's findings [14].

B. Research Questions

To begin with, research questions were developed based on the objectives of this review and insights from relevant

previous studies. The primary questions guiding this SLR are stated in the introduction section. These questions were formulated by established methodologies in prior SLRs and aimed at addressing critical gaps identified in the literature. This process ensures that the review is focused and addresses significant issues in information security awareness maturity models.

C. Identification Phase

Next, in conducting this systematic literature review (SLR), a comprehensive search strategy was employed to ensure the inclusion of relevant literature on cyber security, information security, maturity models and awareness programs. The main keywords identified were "cyber security", "information security", "maturity", "awareness", “model” and “framework”. To diversify these keywords, synonyms and related terms were incorporated, such as "cybersecurity maturity," "information security maturity," "security awareness," and "cybersecurity awareness." This process involved consulting online thesauruses, previous studies, and expert opinions to enrich the keyword list.

The search strategy utilized Boolean operators, truncation, and phrase searching across two primary databases: Scopus and IEEE Xplore. These databases were chosen due to their extensive coverage of high-quality research in computer science and information security. The search string used in Scopus and IEEE Xplore is detailed as follows; ("cyber security maturity" OR "cybersecurity maturity" OR "information security maturity" OR "cyber security awareness" OR "cybersecurity awareness" OR "information security awareness" OR "security awareness" OR “security maturity”) AND ("maturity framework" OR "maturity model" OR "awareness framework" OR "awareness model" OR "capability model" OR "capability framework"). From these searches, 209 articles were retrieved from Scopus, and 74 articles were retrieved from IEEE Xplore.

D. Screening Phase

The screening process involved several steps to filter out articles that did not meet the inclusion criteria. The criteria for selecting suitable articles were based on publication date (2019-2024), language (English), and relevance to the field of computer science research. This period was chosen to ensure the inclusion of the most recent and relevant studies, as the field of information security evolves rapidly.

The initial search resulted in 283 articles from both databases. After removing 57 duplicate articles, 226 articles remained. These were further filtered by reviewing titles and abstracts, excluding an additional 55 articles that did not align with the inclusion criteria, which involved relevance to cyber security maturity models and awareness programs. This rigorous screening left 80 articles for full-text review. Following a detailed assessment of these articles, 25 were selected for the final review based on their empirical evidence and significant contributions to the research questions posed in this SLR.

The decision to focus on articles published between 2019 and 2024 was guided by the need to include the most recent advancements and discussions in the field. This period captures the latest trends, technologies, and methodologies in information security maturity and awareness. Limiting the review to English language publications ensured consistency in comprehension and analysis. To ensure the rigor and reliability of the findings, the analysis solely encompassed peer-reviewed scholarly articles from reputable journals and conferences with a publication date within the last six years. By adhering to these stringent criteria, this investigation aimed to present a comprehensive and up-to-date understanding of the contemporary landscape of ISA.

E. Eligibility Phase

Eligibility is the third process where the authors manually monitored the retrieved articles to ensure all the remaining articles after the screening process align with the established criteria. This process involved an in-depth review of the full texts of the articles to confirm their relevance to the maturity model for awareness in information security, specifically focusing on maturity levels, dimensions or areas, and the applicable sectors or organizations.

This meticulous process excluded 55 articles. Articles were removed if they primarily focused on vulnerabilities rather than maturity models, emphasized general cybersecurity without addressing maturity levels or stages, or were centered on sectors unrelated to information security. The process utilized for screening and evaluating the records is depicted in the PRISMA flow diagram in Fig. 1. After this thorough eligibility assessment, 25 articles were selected for inclusion in the SLR.

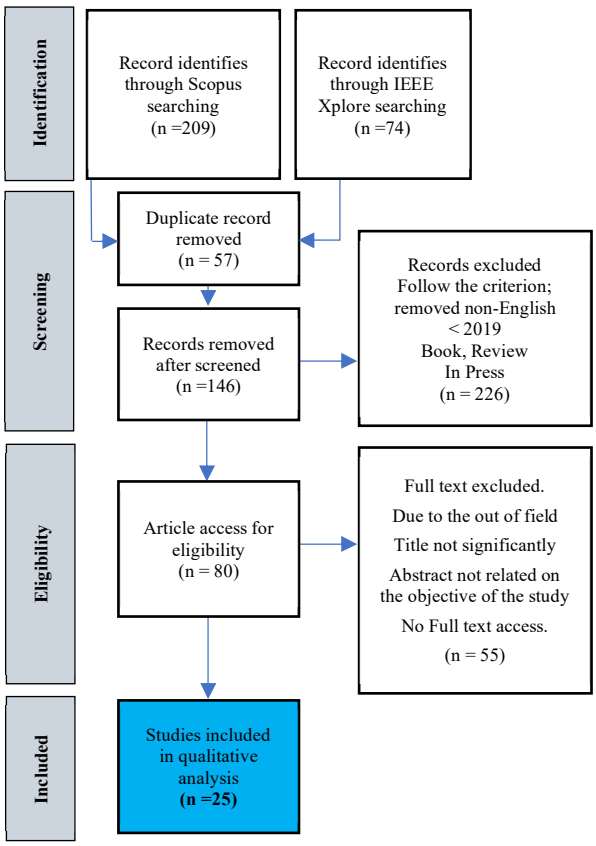

Fig. 1 Flow diagram of the proposed searching study

These articles provided substantial insights into various maturity models for information security awareness, detailing different maturity levels, stages, and dimensions such as risk, compliance, policy, and human factors. The selected articles also covered a range of sectors, including healthcare, public sector, SMEs, and higher education, providing a comprehensive overview of the current state of information security awareness maturity models across different organizational contexts.

F. Quality Assessment

The quality assessment was guided by the criteria established by [15], which consists of six key questions aimed at evaluating various aspects of each study. The measurement tool employed for this quality assessment was a structured evaluation matrix based on the criteria set forth by [15]. The six criteria used to assess the quality of the articles were as follows:

a. Q1: Is the purpose of the study clearly stated? This criterion examines whether the study's objectives and goals are explicitly mentioned, providing a clear understanding of what the study aims to achieve.
b. Q2: Is the interest and usefulness of the work clearly presented? This evaluates whether the study's relevance and practical applications are well-articulated, highlighting its importance in the field.
c. Q3: Are the concepts of the approach clearly defined? This checks if the theoretical framework, methodologies, and key concepts are adequately explained, ensuring that the study's approach is comprehensible.
d. Q4: Do the findings address the stated objectives of the study? This assesses whether the results and conclusions are aligned with the initial objectives, indicating the study's effectiveness in meeting its goals.
e. Q5: Is the work compared and measured with other similar work? This criterion looks at whether the study engages in comparative analysis with existing research, providing context and demonstrating its contribution to the field.
f. Q6: Are the limitations of the work clearly mentioned? This examines whether the study acknowledges its own limitations, which is crucial for transparency and guiding future research.

The quality assessment was carried out by the primary author with the assistance of a co-author. Both reviewers meticulously evaluated each article based on the six criteria. For each criterion met, a score of 'Yes' (1.0 point) was assigned. If a criterion was partially met, a score of 'Partial' (0.5 points) was given, and for unmet criteria, a score of 'No' (0 points) was recorded.

Based on the quality assessment criteria, each article was evaluated against six specific questions to determine its suitability for inclusion in the systematic literature review (SLR). Articles were deemed of high quality and included in the SLR if they achieved a total score of 3.0 or above, indicating that at least 50% of the quality criteria were met. This threshold ensures that only robust and methodologically sound studies are considered. Table I presents the updated results, including the total score for each article. All 25 articles scored above the threshold, with most achieving the maximum score, demonstrating their strong alignment with the assessment criteria.

TABLE I
QUALITY ASSESSMENT SHORTLISTED ARTICLES

Reference	Q1	Q2	Q3	Q4	Q5	Q6	Total Score
A01	1	1	1	1	1	1	6
A02	1	1	1	1	1	1	6
A03	1	1	1	1	1	1	6
A04	1	1	1	1	1	1	6
A05	1	1	1	1	1	1	6
A06	1	1	1	1	1	1	6
A07	1	1	1	1	1	1	6
A08	1	1	1	1	1	1	6
A09	1	1	1	1	1	0.5	5.5
A10	1	1	1	1	1	0.5	5.5
A11	1	1	1	1	0.5	1	5.5
A12	1	1	1	1	1	0.5	5.5
A13	1	1	1	1	1	1	6
A14	1	1	1	1	1	1	6
A15	1	1	1	1	1	1	6
A16	1	1	1	1	1	1	6
A17	1	1	1	1	1	1	6
A18	1	1	1	1	1	1	6
A19	1	1	1	1	1	1	6
A20	1	1	1	1	1	0.5	5.5
A21	1	1	1	1	1	1	6
A22	1	1	1	1	1	1	6
A23	1	1	1	1	1	1	6
A24	1	1	1	1	1	1	6
A25	1	1	1	1	1	1	6

III. RESULTS AND DISCUSSION

This section aims to synthesize the findings from selected literature on Information Security Awareness (ISA) maturity models. This study addresses the following research questions: What are the existing maturity models for information security awareness? What are the common dimensions and levels included in these models? What are the identified gaps and limitations in current ISA maturity models? This discussion highlights findings from 25 articles to provide a comprehensive overview of current models, focus areas and the standards or frameworks guiding the development.

A. Existing Maturity Model for ISA

The ISA maturity models identified in the literature encompass diverse sectors, objectives, and methodologies. These models range from those designed for specific industries, such as healthcare and finance, to more generalized frameworks applicable across different organizational contexts. Key models include the Maturity Model for Information Security Awareness (MMISA) by [16], which is tailored for Hungarian organizations and emphasizes strong risk assessment mechanisms and organizational structure. Another significant model is the Balanced Information Security Maturity Model (BISM) by [17], which integrates controls from ISO/IEC 27001 and O-ISM3, offering a flexible and adaptable approach to ISMS maturity.

In addition, several models focus on specific sectors, such as the Cybersecurity Maturity Model for the Protection and Privacy of Personal Health Data by [18], which addresses the unique challenges in healthcare organizations, and the Cyber Security Maturity Assessment Framework for Technology

Startups by [9], designed to assess and enhance cybersecurity maturity in technology startups. Other models, like the Holistic Evaluation Model for Cybersecurity Awareness Programs by [19], offer comprehensive assessments that integrate knowledge and behavioral aspects of cybersecurity awareness. This model is particularly noteworthy for using machine learning (ML) algorithms to identify risky behaviors and recommend effective CSA programs.

Furthermore, the Requirements Engineering Security Maturity Model (RESMM) by [20] focuses on secure requirements engineering, while the National Cyber Security Maturity Model by [21] provides a comprehensive evaluation of cyber security maturity at the national level.

The MMISA model by [16] is robust in providing practical controls and audit evidence, supporting risk assessment and organizational structure in ISA. However, its regional focus on Hungary limits its applicability in broader contexts. This model's strength lies in its detailed and structured approach, making it ideal for organizations seeking a comprehensive evaluation of maturity levels. The BISM model by [17] stands out for its flexibility and adaptability. Integrating ISO/IEC 27001 and O-ISM3 controls provides a balanced approach to ISMS maturity. However, while the model shows high compliance values, it requires further validation across diverse organizational contexts to confirm its effectiveness beyond the initial study.

Alharbi's [19] holistic model is innovative in combining passive (survey-based) and active (log file-based) data collection techniques. Using ML algorithms to analyze behavior adds a layer of sophistication to the model. Nonetheless, relying on ML may limit its accessibility for organizations lacking advanced technical capabilities. Further, the need for empirical validation in real-world environments is a critical limitation. The RESMM [20] offers a well-structured framework for secure requirements engineering, making it a valuable tool for software development organizations. However, its narrow focus on the software industry may limit its applicability.

In contrast, the National Cyber Security Maturity Model by [21] provides a more generalized approach, focusing on cyber security at the national level. While comprehensive in scope, its reliance on expert opinions and the need for empirical validation in broader contexts are significant limitations. Other models, such as the Cybersecurity Maturity Model to Prevent Cyberattacks on Web Applications by [22] emphasize specific domains, in this case, web applications. This model integrates NIST and ISO 27032 standards, and its automated assessment tool makes it highly practical. However, like other models, its broader applicability requires further testing in diverse settings.

The Cybersecurity Culture Maturity and Deriving Verifiable Improvement Measures model by [23] addresses the human factors in cybersecurity, focusing on improving cybersecurity culture. While effective in enhancing specific dimensions of cybersecurity culture, the reliance on self-reported data may introduce biases, and the model's applicability in different organizational contexts needs exploration. Similarly, Fertig et al.'s [24] model for Maturity Model for Information Security Awareness uses rigorous statistical methods to identify strengths and weaknesses in ISA. Although the model is well-structured, its sample size and specific organizational contexts may limit the generalizability of its findings.

In the healthcare sector, Barnes and Daim's [14] Information Security Maturity Model for Healthcare Organizations provides a hierarchical decision model (HDM) that helps prioritize resources to mitigate significant threats. While this model effectively addresses healthcare-specific challenges, broader validation across different healthcare settings must confirm its applicability.

The Maturity Level Assessments of Information Security Controls by [25] focuses on improving the accuracy of practitioners' security maturity level assessments. Although it identifies critical gaps in assessment capabilities, the model's reliance on hypothetical scenarios may not fully capture real-world complexities. Other models, such as the Cyber Security Maturity Model Capability at The Airports by [26], highlight the sector-specific needs of airports, emphasizing the importance of addressing significant gaps in cybersecurity practices. While insightful, the study's geographic focus on Australia may limit its generalizability.

The Data Leakage Prevention Maturity model by [27] effectively adapts the C2M2 framework for data leakage prevention (DLP) in the financial sector. Its holistic approach demonstrates potential, though broader validation across different sectors would enhance its generalizability. The Cybersecurity Maturity Model for Providing Services in the Financial Sector by [28] successfully integrates cloud security and privacy capabilities, showing high acceptance levels in pilot studies. However, its applicability beyond the financial sector in Peru needs exploration.

When comparing the effectiveness and applicability of these models, it becomes evident that no single model can address all organizational needs. The BISM model [17] and the MMISA model [16] provide structured approaches suitable for organizations seeking detailed assessments, while the holistic model by [19] and the cybersecurity culture model by [23] offer more flexible approaches that address behavior and culture.

Sector-specific models, such as those designed for healthcare [14], [18] and financial services [27], [28], provide valuable insights tailored to the unique challenges of these industries. However, their applicability outside these sectors remains a challenge. The models focusing on national and sectoral levels, such as the National Cyber Security Maturity Model [21] and the Cyber Security Maturity Model Capability at The Airports [26], highlight the need for broader validation to ensure their effectiveness across different contexts.

The existing models focus on various aspects of information security awareness, including risk assessment, policy compliance, cultural transformation, and technological integration. These focus areas are illustrated in Table II, which highlights the summary concentration of these areas and guides standard across the reviewed models. The models are guided by several standards and frameworks that ensure their effectiveness and applicability. Most reviewed models incorporate internationally recognized standards such as ISO/IEC 27001, NIST frameworks, and COBIT. For instance, the BISM model utilizes ISO/IEC 27001 and O-ISM3, while the RESMM is based on CMMI v1.3 and Sommerville's practices [20]. The National Cyber Security Maturity Model

incorporates ISO/IEC 27001:2013 and the NIST SP800 framework, emphasizing its comprehensive approach [21].

The MMISA model [16] is robust in providing practical controls and audit evidence, supporting risk assessment and organizational structure in ISA. However, its focus on Hungarian organizations limits its broader applicability. Similarly, the BISM model [17] effectively merges detailed controls from ISO/IEC 27001 with process-based approaches from O-ISM3, making it flexible across diverse contexts. However, it requires further validation in different settings.

The reviewed maturity models for information security awareness provide various approaches, each with distinct strengths and weaknesses. While some models offer flexibility and adaptability across various organizational contexts, others are more rigid and tailored to specific sectors or regions. The BISM and MMISA models stand out for their structured approaches, while Alharbi's [19] holistic model and the cybersecurity culture model by [23] emphasize behavior and culture. Sector-specific models address unique challenges but require further validation to ensure broader applicability. Integrating recognized standards like ISO/IEC 27001 and NIST frameworks ensures robustness and applicability. However, the models' effectiveness often depends on their validation and adaptability.

B. Dimensions and Levels

The analysis in this sub-section addresses the research question: What are the standard dimensions and levels included in these models? Through a synthesis of these models, the discussion will highlight strengths, weaknesses, and applicability, drawing on the content from the selected articles. The maturity models reviewed in the literature reveal several recurring dimensions critical to assessing ISA maturity. These dimensions include risk management, organizational culture, training programs, policy compliance, and technical measures. These dimensions serve as foundational elements in guiding organizations toward improving their information security awareness and overall security posture.

Risk management is a predominant dimension across multiple models. For instance, the Maturity Model for Information Security Awareness (MMISA) by [16] and the Cybersecurity Maturity Model to Prevent Cyberattacks on Web Applications by [22] both emphasize risk management as a critical factor in determining maturity. These models underscore the importance of identifying, assessing, and mitigating risks as essential components of a robust ISA framework. Similarly, the SME Information Security Maturity Model (SME ISMM) by [29] and the Cyber Security Maturity Assessment Framework (CMAF) by [30] incorporate risk management as a core dimension, highlighting its role in establishing a secure and resilient information security environment.

Organizational culture is another key dimension in the ISA maturity models. The Holistic Evaluation Model for Cybersecurity Awareness Programs by [19] and the Cybersecurity Culture Maturity model by [23] emphasize the role of organizational culture in fostering a security-conscious environment. These models recognize that a culture of awareness and commitment to security is essential for successfully implementing and sustaining ISA practices. Organizational support is also a significant dimension in models such as [14] and [24], where leadership and organizational commitment are pivotal in driving security awareness and compliance.

Training programs are frequently highlighted as essential for improving ISA maturity. Models like the Cybersecurity Maturity Model for the Protection and Privacy of Personal Health Data by [18] and the Maturity Model for Information Access Management by [35] focus on developing and implementing effective training programs to enhance awareness and behavior change among employees. The importance of continuous education and skill development is further emphasized in models like [26] and [27], which both include training as a critical dimension for ensuring that employees are equipped to handle evolving security challenges.

Policy compliance and technical measures are also consistently identified as vital dimensions in the reviewed models. The Balanced Information Security Maturity Model (BISM) by [17] and the National Cyber Security Maturity Model by [21] include policy compliance as a key component, reflecting the necessity of adhering to established standards and regulations to achieve higher maturity levels. Technical measures, including security controls, incident response, and access management, are equally emphasized in models such as [34] and [38]. These models stress the importance of implementing robust technical solutions to protect organizational assets and ensure compliance with security standards.

The maturity levels across these models vary in terminology but generally follow a progression from basic or initial stages to advanced or optimized stages. This progression reflects the increasing complexity and effectiveness of the ISA measures implemented as organizations move up the maturity ladder. In many models, the initial stages are characterized by ad hoc or non-existent practices. For instance, the SME ISMM by [29] and the Security Maturity Model by [31] describe the early stages as "Non-existent" or "Ad hoc," where organizations have minimal or inconsistent ISA practices in place. Similarly, the Cyber Security Maturity Model Capability at The Airports by [26] and the Cybersecurity Maturity Model to Prevent Cyberattacks on Web Applications by [22] start with basic levels that signify limited security awareness and controls.

As organizations progress through the maturity levels, the models introduce more structured and defined processes. The CMAF by [30] and the Cybersecurity Maturity Model for Providing Services in the Financial Sector by [28] include stages like "Managed" and "Defined," where processes become standardized, documented, and more consistently applied across the organization. These levels indicate a growing commitment to ISA, with organizations actively working to embed security awareness into their operations. The advanced stages of maturity are often described as "Optimized" or "Continuously Improved," where organizations have fully integrated ISA practices into their culture and operations. For example, [38] and [24] culminate in stages where ISA is maintained continuously evaluated and enhanced to adapt to new threats and challenges. These stages reflect a proactive approach to ISA, where organizations prioritize ongoing improvement and resilience.

Each dimension and maturity level offers specific strengths and weaknesses depending on the context of the organization and the maturity model being applied. For example, risk management as a dimension is universally recognized as critical for ISA. However, the effectiveness of this dimension often depends on the organization's ability to accurately assess and mitigate risks. Models like the MMISA by [16] and the CMAF by [30] that emphasize risk management provide robust frameworks for identifying and addressing risks, but they may require significant resources and expertise to implement effectively.

TABLE II
SUMMARY OF EXISTING MATURITY MODEL

Model Name	Areas	Standards/Model	Ref
MMISA	Public sector, SMEs, healthcare, higher education	SANS Maturity Model, ISO/IEC standards	[16]
BISM	Various organizations	ISO/IEC 27001:2013, O-ISM3	[17]
Holistic Evaluation Model for CSA	General work environments	National frameworks, ISO, HIPAA, NIST	[19]
RESMM	Software development	CMMI v1.3, Sommerville's practices	[20]
National Cyber Security Maturity Model	Public sector	ISO/IEC 27001:2013, NIST SP800 framework	[21]
CMAF	Public sector	NIS Directive, ISO/IEC 27001	[30]
SME ISMM	SMEs	ISO/IEC 27002	[29]
Security Maturity Model	Public sector, telecommunications	ISM3, ISO/IEC 27001	[31]
Cyber Security Maturity for Startups	Technology startups, FinTech	ISO/IEC 27001, NIST, COBIT, C2M2	[32]
National Cybersecurity Maturity	National level	CERT-RMM, C2M2, ISO/IEC 27001	[33]
Cyber Security Maturity for Startups	Technology startups	NIST, ISO 27001, COBIT 5, C2M2, CMMI	[9]
Cyber Security Maturity at Airports	Airports	CMMC	[26]
Cybersecurity Maturity Assessment Design	Critical infrastructures	NIST CSF, CIS Controls v8, ISO/IEC 27002	[34]
Cybersecurity for Financial Sector	Financial sector	NIST framework	[28]
Cybersecurity for Health Data	Health sector	C2M2,	[18]
Cybersecurity for Web Applications	Web applications	NIST, ISO 27032	[22]
Cybersecurity Culture Maturity	General organizations	IPCA framework	[23]
Developing ISA	Various organizations	Integrated Behavioral Model, Rasch model	[24]
IS Maturity for Healthcare	Healthcare	HDM	[14]
Maturity Level Assessments	Various organizations	COBIT, ISO/IEC 27002	[25]
Information Access Management	IT service providers	ISO/IEC 27001:2022, CMMI	[35]
IS Security in Private Banks	Private banks	SSE-CMM, ISO/IEC 27001	[36]
Data Leakage Prevention Maturity	Financial sector	C2M2	[27]
SCSAM-Elderly	Elderly population	Security Awareness Model, ISAPM	[37]
M2HCS	Healthcare	NIST, ISO/IEC 27000 series	[38]

Organizational culture is a powerful driver of ISA maturity, as seen in models like the Holistic Evaluation Model by Alharbi [19] and the Cybersecurity Culture Maturity model by [23]. A strong security culture can significantly enhance the effectiveness of ISA initiatives. However, changing organizational culture can be challenging and requires sustained effort from leadership and management.

Training programs are essential for developing and maintaining ISA, but their effectiveness can vary depending on how well they are tailored to the organization's needs. Models like the Cybersecurity Maturity Model for the Protection and Privacy of Personal Health Data by [18] highlight the importance of customized training programs that address specific industry challenges. However, the success of these programs depends on the organization's commitment to ongoing education and the ability to measure and improve training outcomes.

Policy compliance and technical measures are critical for ensuring that ISA practices are aligned with industry standards and effectively protect organizational assets. Models like the BISM by [17] and the National Cyber Security Maturity Model by [21] offer comprehensive frameworks for achieving compliance and implementing technical controls. However, these dimensions may require significant investment in technology and expertise, which can be a barrier for smaller organizations.

Most models structure the progression through maturity levels well, with clear indicators of advancement. However, the terminology and specific criteria for each level can vary significantly between models, which may lead to confusion or difficulties in comparing the maturity levels across different frameworks. Additionally, reaching the highest maturity levels often requires substantial resources, making achieving these stages challenging for some organizations.

The standard dimensions and maturity levels analysis across various ISA maturity models reveals a broad consensus on the key elements necessary for enhancing information security awareness. Risk management, organizational culture, training programs, policy compliance, and technical measures are integral to building a robust ISA framework. The maturity levels provide a structured pathway for organizations to develop and refine their ISA practices, although the specific terminology and criteria can vary between models. While these models offer valuable guidance for improving ISA, their effectiveness depends on the organization's ability to implement and sustain the necessary practices.

C. Gaps and Limitations in Current Models

This sub-section aims to identify and analyze the gaps and limitations in current Information Security Awareness (ISA) maturity models, as highlighted in the literature. This analysis seeks to answer the research question: What gaps and limitations are identified by the current ISA maturity models? By synthesizing the findings from all 25 articles, the discussion will explore the implications of these gaps and limitations and offer comparisons across different models regarding their effectiveness and applicability.

A consistent theme across the reviewed models is the lack of tailored ISA maturity models for specific organizational contexts. For instance, while the Maturity Model for Information Security Awareness (MMISA) by [16] Its structure is robust and predominantly focused on Hungarian organizations, limiting its applicability to other regions or industries. Similarly, the Balanced Information Security Maturity Model (BISM) by [17] is designed with flexibility in mind but may not fully address the unique needs of smaller organizations, such as SMEs or start-ups. These models often lack the specificity needed for practical implementation in varied organizational environments, such as technology start-ups or financial institutions [9], [28].

Another significant limitation is the reliance on broad and generic frameworks that do not adequately address sector-specific challenges or emerging threats. For example, [19] holistic model, while comprehensive, does not provide detailed guidance for specific sectors, such as healthcare or financial services. The Security Maturity Model by [31] and the Cybersecurity Maturity Assessment by [34] similarly lack the granularity needed to address the nuances of different industries, resulting in models that may be too generalized to be fully effective in all contexts.

The reliance on self-reported data and expert opinions is another pervasive issue, which can introduce potential biases and variability in the reliability of these models. For instance, the National Cyber Security Maturity Model by [21] and the Cyber Security Maturity Model Capability at The Airports by [26] both depend heavily on expert judgment. While expert insights are valuable, they may vary significantly depending on the expertise and perspective of the individuals involved, potentially leading to inconsistencies in applying these models. Ensuring empirical validation through additional quantitative or empirical testing could enhance the robustness and generalizability of the findings.

Moreover, many models fail to integrate both technical and managerial aspects comprehensively. The Requirements Engineering Security Maturity Model (RESMM) by [20] and the Maturity Model for Information Access Management by [35] primarily focus on technical measures without fully incorporating the crucial behavioral and cultural dimensions for effective ISA. This lack of a holistic approach can result in gaps in implementing ISA practices, where adequate management practices or employee engagement do not support technical solutions.

Furthermore, several models lack practical improvement measures and risk quantification. This gap is particularly evident in models designed for smaller or more agile organizations, such as the SME ISMM by [29] and the Cyber Security Maturity Model for Technology Startups by [32]. These models often struggle to provide actionable steps for organizations to progress through maturity, especially when resources are limited. Additionally, the Cybersecurity Maturity Model to Prevent Cyberattacks on Web Applications by [22] highlights the need for improved risk assessment capabilities within these frameworks, as many existing models do not adequately quantify the risks associated with different maturity levels.

The identified gaps and limitations have several important implications for developing and applying ISA maturity models. Firstly, organizations aiming to implement or improve their ISA maturity models must consider adopting more tailored frameworks that are specific to their industry and organizational context. For instance, healthcare organizations might benefit from models like the Information Security Maturity Model for Healthcare Organizations by [14], designed to address the unique security challenges in the healthcare sector. However, this model requires further refinement to integrate the latest technological advancements and fully address emerging threats.

Additionally, integrating both technical and behavioral dimensions is essential for creating a comprehensive approach to ISA maturity. Models focusing solely on technical measures without addressing the human factors involved will likely fall short of achieving sustained improvements in information security awareness. Therefore, models such as the Developing a Maturity Model for Information Security Awareness by [24] and the Cybersecurity Maturity Model for the Protection and Privacy of Personal Health Data by [18] should be further developed to include more robust behavioral assessments alongside technical controls.

For regulatory bodies and policymakers, the findings suggest the need to promote the development of standardized cybersecurity frameworks that are flexible enough to accommodate different organizational sizes and sectors. These frameworks should emphasize compliance with established standards such as ISO/IEC 27001 while also encouraging the adoption of advanced technologies like machine learning for data analysis and risk assessment, as seen in models like the CMAF by [30]. Moreover, policymakers should encourage collaboration between the public and private sectors to enhance the development and implementation of effective ISA maturity models adaptable to various organizational contexts.

Developing ISA maturity models specifically tailored for the public sector is crucial due to the unique challenges and responsibilities these organizations face. Public sector entities often handle sensitive information and are subject to stringent regulatory requirements. Therefore, a maturity model that integrates comprehensive risk management, policy compliance, and regular training programs is essential. The use of an updated version of the ISO 27000 series can provide a robust framework for ensuring that public sector organizations maintain high standards of information security awareness and preparedness [21]. The importance of using updated versions of standards and frameworks, such as the ISO 27000 series, cannot be overstated. As cyber threats evolve, ISA maturity models must incorporate the latest best practices and guidelines. This ensures that organizations are well-equipped to handle new and emerging threats and maintain high security and resilience [32], [33].

IV. Conclusion

This systematic literature review has identified and evaluated various Information Security Awareness (ISA) maturity models, highlighting strengths and limitations. Key findings indicate that while these models offer valuable frameworks for enhancing ISA, many fail to meet the specific needs of different organizational contexts. Several models are designed for broad applicability but lack the specificity for healthcare, finance, and the public sector. Additionally, a significant gap exists in the comprehensive integration of technical and managerial aspects, which is essential for a holistic approach to ISA. The review also points out the heavy reliance on self-reported data and expert opinions in numerous models, potentially introducing biases and compromising the reliability of assessments. This reliance underscores the need for more empirical validation to ensure the robustness and generalizability of these models. Furthermore, several models do not sufficiently address the need for practical improvement measures and risk quantification, particularly for smaller or more agile organizations like SMEs and technology start-ups.

These findings are significant as they guide the future development of ISA maturity models. Addressing identified gaps, such as the need for sector-specific tailoring, comprehensive integration of technical and managerial aspects, and rigorous empirical validation, can lead to more effective and adaptable models. This is particularly crucial for the public sector, where the unique challenges of regulatory compliance, resource constraints, and safeguarding sensitive information necessitate a tailored approach to ISA maturity. An appropriately designed maturity model for the public sector can significantly enhance security practices and maintain public trust. Moreover, adopting updated international standards, such as the ISO 27000 series, is vital. These standards offer a current and globally recognized foundation for information security management, ensuring alignment with the latest best practices. Integrating these standards into ISA maturity models will improve effectiveness and relevance in a rapidly evolving cybersecurity landscape.

In conclusion, this review emphasizes the necessity for continuous refinement and innovation in ISA maturity models. Developing models that are tailored, empirically validated, and aligned with updated standards can significantly enhance security posture and better protect organizational assets across all sectors.

Acknowledgment

The authors gratefully acknowledge the financial assistance provided by the Faculty of Computer Science and Information Technology (FCSIT) of the University Putra Malaysia. Additionally, sincere appreciation is extended to the Public Service Department for sponsoring this study, which has greatly contributed to its realization.

References

[1] E. A. Metwally et al., "Hacking Human: Hacking the Weakest Link in the Security Chain," *Medicon Engineering Themes,* vol. 2, no. 4, pp. 45-58, 2022.

[2] T. Ncubukezit, "Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses," *International Conference on Cyber Warfare and Security*, vol. 17, no. 1, pp. 395–403, Mar. 2022, doi: 10.34190/iccws.17.1.51.

[3] G. Klein and M. Zwilling, "The Weakest Link: Employee Cyber-Defense Behaviors While Working from Home," *Journal of Computer Information Systems*, vol. 64, no. 3, pp. 408–422, Jun. 2023, doi:10.1080/08874417.2023.2221200.

[4] M. Schmid and S. Pape, "A Structured Comparison of the Corporate Information Security Maturity Level," *ICT Systems Security and Privacy Protection*, pp. 223–237, 2019, doi: 10.1007/978-3-030-22312-0_16.

[5] M. Bitzer, B. Häckel, D. Leuthe, J. Ott, B. Stahl, and J. Strobel, "Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities," *Computers & Security*, vol. 125, p. 103050, Feb. 2023, doi: 10.1016/j.cose.2022.103050.

[6] R. Adriko and J. R. C. Nurse, "Cybersecurity, cyber insurance and small-to-medium-sized enterprises: a systematic Review," *Information & Computer Security*, Jun. 2024, doi: 10.1108/ics-01-2024-0025.

[7] M. A. Rizal and B. Setiawan, "Information Security Awareness Literature Review: Focus Area for Measurement Instruments," *Procedia Computer Science*, vol. 234, pp. 1420–1427, 2024, doi:10.1016/j.procs.2024.03.141.

[8] A. K. Gwenhure and F. Sapty Rahayu, "Gamification of Cybersecurity Awareness for Non-IT Professionals: A Systematic Literature Review," *International Journal of Serious Games*, vol. 11, no. 1, pp. 83–99, Mar. 2024, doi: 10.17083/ijsg.v11i1.719.

[9] M. N. Y. Marican, S. A. Razak, A. Selamat, and S. H. Othman, "Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review," *IEEE Access*, vol. 11, pp. 5442–5452, 2023, doi: 10.1109/access.2022.3229766.

[10] N. Ukeje, J. Gutierrez, and K. Petrova, "Information security and privacy challenges of cloud computing for government adoption: a systematic review," *International Journal of Information Security*, vol. 23, no. 2, pp. 1459–1475, Jan. 2024, doi: 10.1007/s10207-023-00797-6.

[11] S. Chaudhary, V. Gkioulos, and S. Katsikas, "A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises," *Computer Science Review*, vol. 50, p. 100592, Nov. 2023, doi: 10.1016/j.cosrev.2023.100592.

[12] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, p. n71, Mar. 2021, doi:10.1136/bmj.n71.

[13] H. A. Mohamed Shaffril, S. F. Samsuddin, and A. Abu Samah, "The ABC of systematic literature review: the basic methodological guidance for beginners," *Quality & Quantity*, vol. 55, no. 4, pp. 1319–1346, Oct. 2020, doi: 10.1007/s11135-020-01059-6.

[14] B. Barnes and T. Daim, "Information Security Maturity Model for Healthcare Organizations in the United States," *IEEE Transactions on Engineering Management*, vol. 71, pp. 928–939, 2024, doi:10.1109/tem.2021.3139836.

[15] A. Abouzahra, A. Sabraoui, and K. Afdel, "Model composition in Model Driven Engineering: A systematic literature review," *Information and Software Technology*, vol. 125, p. 106316, Sep. 2020, doi: 10.1016/j.infsof.2020.106316.

[16] A. Kő, G. Tarján, and A. Mitev, "Information security awareness maturity: conceptual and practical aspects in Hungarian organizations," *Information Technology & People*, vol. 36, no. 8, pp. 174–195, Jul. 2023, doi: 10.1108/itp-11-2021-0849.

[17] M. A. H. Almekhlafi, "A Balanced Information Security Maturity Model based on ISO/IEC 27001: 2013 and O-ISM3," *Int. J. Innov. Sci. Res. Technol.*, vol. 8, no. 6, pp. 2444-2459, Jun. 2023.

[18] A. J. S. Rojas, E. F. P. Valencia, J. Armas-Aguirre, and J. M. M. Molina, "Cybersecurity maturity model for the protection and privacy of personal health data," *2022 IEEE 2nd International Conference on Advanced Learning Technologies on Education & Research (ICALTER)*, pp. 1–4, Nov. 2022, doi:10.1109/icalter57193.2022.9964729.

[19] T. Alharbi, "A Holistic Evaluation Model for Information Security Awareness Programs in Work Environment," *2023 Eighth International Conference On Mobile And Secure Services (MobiSecServ)*, pp. 1–4, Nov. 2023, doi:10.1109/mobisecserv58080.2023.10329041.

[20] M. Niazi, A. M. Saeed, M. Alshayeb, S. Mahmood, and S. Zafar, "A maturity model for secure requirements engineering," *Computers & Security*, vol. 95, p. 101852, Aug. 2020, doi:10.1016/j.cose.2020.101852.

[21] M. Omrani, M. Shafiee, and S. Khorsandi, "A Model to Measure Cyber Security Maturity at the National Level," *2023 31st*

International Conference on Electrical Engineering (ICEE), pp. 110–116, May 2023, doi: 10.1109/icee59167.2023.10334826.

[22] E. Arenas, J. Palomino, and J.-P. Mansilla, "Cybersecurity Maturity Model to Prevent Cyberattacks on Web Applications Based on ISO 27032 and NIST," *2023 IEEE XXX International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, pp. 1–8, Nov. 2023, doi: 10.1109/intercon59652.2023.10326028.

[23] P. Dornheim and R. Zarnekow, "Determining cybersecurity culture maturity and deriving verifiable improvement measures," *Information & Computer Security*, vol. 32, no. 2, pp. 179–196, Oct. 2023, doi:10.1108/ics-07-2023-0116.

[24] T. Fertig, A. Schütz, and K. Weber, "Developing a maturity model for information security awareness using a polytomous extension of the Rasch model," *Hawaii International Conference on System Sciences 2023 (HICSS-56)*, 2023.

[25] C. Schmitz, M. Schmid, D. Harborth, and S. Pape, "Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities," *Computers & Security*, vol. 108, p. 102306, Sep. 2021, doi: 10.1016/j.cose.2021.102306.

[26] O. Malhotra, S. Dey, E. Foo, and M. Helbig, "Cyber Security Maturity Model Capability at The Airports," *ACIS 2021 Proceedings,* vol. 55, 2021.

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

[28] J. G. Alayo, P. N. Mendoza, J. Armas-Aguirre, and J. M. Molina, "Cybersecurity maturity model for providing services in the financial sector in Peru," *2021 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI)*, pp. 1–4, Sep. 2021, doi:10.1109/coniiti53815.2021.9619733.

[29] B. Yigit Ozkan and M. Spruit, "Addressing SME Characteristics for Designing Information Security Maturity Models," *Human Aspects of Information Security and Assurance*, pp. 161–174, 2020, doi:10.1007/978-3-030-57404-8_13.

[30] G. Drivas, A. Chatzopoulou, L. Maglaras, C. Lambrinoudakis, A. Cook, and H. Janicke, "A NIS Directive Compliant Cybersecurity Maturity Assessment Framework," *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC),* Jul. 2020, doi: 10.1109/compsac48688.2020.00-20.

[31] O. M. M. Al-Matari, I. M. A. Helal, S. A. Mazen, and S. Elhennawy, "Adopting security maturity model to the organizations' capability model," *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 193–199, Jul. 2021, doi: 10.1016/j.eij.2020.08.001.

[32] A. Selamat, M. N. Y. Marican, S. H. Othman, and S. A. Razak, "An End-To-End Cyber Security Maturity Model For Technology Startups," *2022 IEEE International Conference on Computing (ICOCO)*, pp. 185–190, Nov. 2022, doi:10.1109/icoco56118.2022.10031900.

[33] G. Sharkov, "Assessing the Maturity of National Cybersecurity and Resilience," *Connections: The Quarterly Journal*, vol. 19, no. 4, pp. 5–24, 2020, doi: 10.11610/connections.19.4.01.

[34] I. Bashofi and M. Salman, "Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002," *2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)*, pp. 58–62, Jun. 2022, doi: 10.1109/cyberneticscom55287.2022.9865640.

[35] S. Huamán, L. Ponce, and L. Wong, "Maturity Model for Information Access Management of Peruvian IT Service Providers based on ISO/IEC 27001 and CMMI Security Controls," *2024 35th Conference of Open Innovations Association (FRUCT)*, pp. 259–266, Apr. 2024, doi: 10.23919/fruct61870.2024.10516387.

[36] T. Shimels and L. Lessa, "Maturity of information systems security in selected private Banks in Ethiopia," *2021 International Conference on Information and Communication Technology for Development for Africa (ICT4DA)*, pp. 184–189, Nov. 2021, doi:10.1109/ict4da53266.2021.9672221.

[37] N. A. Azam, A. Geogiana Buja, M. Y. Darus, and N. Masri Sahri, "SCSAM-Elderly: A New Synergistic Cyber Security Model for the Elderly for IR4.0 Readiness in Malaysia," *2022 IEEE 12th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, pp. 117–122, May 2022, doi: 10.1109/iscaie54458.2022.9794521.

[38] O. O. Akinsanya, M. Papadaki, and L. Sun, "Towards a maturity model for health-care cloud security (M2HCS)," *Information & Computer Security*, vol. 28, no. 3, pp. 321–345, Dec. 2019, doi:10.1108/ics-05-2019-0060.