IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 31 August 2022, accepted 15 November 2022, date of publication 15 December 2022, date of current version 19 January 2023.

Digital Object Identifier 10.1109/ACCESS.2022.3229766

SURVEY

Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review

MOHAMED NOORDIN YUSUFF MARICAN[1], SHUKOR ABD RAZAK[2], (Senior Member, IEEE), ALI SELAMAT[1,3,4,5], (Member, IEEE), AND SITI HAJAR OTHMAN[1], (Member, IEEE)

[1]Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia
[2]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Kuala Terengganu 21300, Malaysia
[3]Malaysia-Japan Institute of Technology, Universiti Teknologi Malaysia, Kuala Lumpur 54100, Malaysia
[4]MaGICX–Media and Game Innovation Centre of Excellence, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia
[5]Faculty of Informatics and Management, University of Hradec Kralove, Hradec Kralove 50003, Czech Republic

Corresponding author: Ali Selamat (aselamat@utm.my)

The author would like to acknowledge the financial support from the Ministry of Higher Education under the Fundamental Research Grant Scheme (FRGS) (FRGS/1/2022/ICT08/UTM/01/1).

ABSTRACT Cybersecurity has gained increasing importance among firms of different sizes and industries due to the significant rise of cyber-attacks over time. Technology startups are particularly vulnerable to cyber-attacks due to the lack of cyber security measures. This is because of limited human capital and financial resources to quantify cyber risks and allocate appropriate investments to cyber security. Technology startups are suppliers and vendors to large organisations such as MNCs, government and financial institutions. They could possibly have a network connection back to the large organisations and might even store confidential information of these large organisations such as financial records, personal data and other proprietary information. As such, with the lack of appropriate cyber security measures, technology startups may be an attack vector for malicious hackers to gain entry to the large organisations. Focusing on technology startups, this study conducted a systematic literature review on cyber security maturity assessment frameworks. This study addressed five research questions on the existing cyber security maturity assessment frameworks in various industries, the target for implementation, cyber security maturity level, shared control domains of these frameworks, and the quantification of the return of cyber security investments. Referring to the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) checklist, a detailed analysis was performed on 24 published research articles (out of 650) from reputable journals and conference proceedings from January 2011 to June 2022. The results revealed the lack of an end-to-end cyber security maturity assessment framework for technology startups. Despite the similarities in the cyber security maturity level for certain frameworks, the results revealed no singular framework that can evaluate the cyber security maturity level of technology startups. The results further revealed the lack of studies on the quantification of the return of cyber security investments in an end-to-end cyber security maturity assessment framework for technology startups. This put the startup in a vulnerable position since management is not able to obtain relevant data on the startup's cyber maturity posture and without such information, they are not able to appropriately justify their security investments to mitigate the evolving cyber risks.

INDEX TERMS Cyber security risk, cyber security maturity, cyber security framework, cyber risk quantification, return of security investment, technology startup.

I. INTRODUCTION

Following the growing connectivity in this digital era, the occurrence of cyber-attacks has continued to increase tremendously. There are different cyber-attacks, such as ransomware attacks, distributed denial of service, phishing, and exploiting vulnerable web and mobile applications. Taking the case of the Southeast Asian region, Singapore encountered a significant increase in cyber-attacks on a weekly basis, with an annual increase of 145% in 2021 [1]. The number of

The associate editor coordinating the review of this manuscript and approving it for publication was Giovanni Merlino.

cyber-attacks has increased inevitably; it is only a matter of time before these attacks occur since anyone with the knowledge of hacking can execute malicious intentions. Being a victim of a cyber-attack is financially taxing which may cost businesses thousands of dollars in recent times [2]. Therefore, it is crucial for the cyber security functions in organisations to have the capability in addressing the potential cyber security threats on a timely basis.

Cyber risks critically affect businesses following widespread cyber-attack cases [3]. Organisations of different sizes, small and medium enterprises (SMEs) or multinational companies (MNCs) are susceptible to these attacks. The size of an SME is no different from a startup [4]. The substantial effects of cyber-attacks in terms of revenues and clients' trust have positioned cyber risks as the top agenda during board meetings. An SME in Singapore reports annual revenue of $100 million or has less than 200 employees [5]. The effects of cyber-attacks are more critical for startups. Startups have limited financial resources to invest in cybersecurity, which makes them more vulnerable to cyber-attacks [6]. Poor security measures put startups at higher risk against these attacks, which have made it particularly challenging for startup founders to gain clients' trust, especially with the rising cases of cyber-attacks [7].

Cyber security issues are no longer an information technology (IT) problem. It has now become a business risk which should be handled with due care at the highest level in the organisation. Most malicious perpetrators have shifted their focus to smaller organisations since they are easier targets than larger organisations [6]. The smaller organisations do not have adequate financial resources to strengthen their information security capabilities in order to protect the business [8]. Smaller organisations like technology startups need to allocate the appropriate investments to implement the required security measures to combat against these cyber threats. The significance of cyber security has propelled the need to establish a specific framework that can help businesses to recognise, prevent, respond, and recover from cyber-attacks [9]. Implementing a cyber security maturity assessment (CSMA) framework equips businesses to deal with cyber threats. Startups demonstrate low cyber security maturity levels due to their lack of cyber security measures, making them susceptible to cyber-attacks [10]. Thus, it is imperative to determine the cyber security maturity level in order to comprehend the current and target maturity level so that startups are able to implement the appropriate cyber security measures to deal with cyber-attacks based on the identified gaps uncovered during the cyber security maturity assessment.

Focusing on technology startups, the current study aims to review the existing CSMA frameworks that are commonly used by cyber security practitioners in the industry. This study specifically examined the comprehensiveness of these frameworks from an end-to-end perspective to assess cyber risks, determining cyber security maturity levels and quantifying the returns of cyber investments for technology startups. Moreover, this study compared the existing and commonly-used cyber security frameworks, underlined their common features and extrapolated the key control domains which can be streamlined to conduct a cyber security maturity assessment for technology startups in a more effective manner. The objective is to provide management with the information to make a more informed decision so that the right amount of investment can be allocated to implement cyber security solutions for the technology startup in order to mitigate the cyber security risks. With the appropriate security measures in place, this will give added protection for the startup to mitigate against cyber-attacks by malicious threat actors.

II. BACKGROUND AND RELATED WORKS

Cybersecurity is one of the most effective methods to counter business risk [3] and is a key determinant in the decision-making process at the organisational level [11]. As of January 2022, there were more than 3,800 startups in Singapore [12]. The Ponemon Institute conducted a survey and revealed that the majority of SMEs experienced cyber-attacks (66%) and data breaches (63%) in the past 12 months [13]. These attacks affected the financial standing, operations, and reputation of organisations. The increasing connectivity and the upsurge of digital transformation initiatives have created a thriving environment for malicious perpetrators, increasing the rate of cyber-attacks. This has called for the need to establish CSMA frameworks and standards in the industry [11].

Various CSMA frameworks are available for cyber security practitioners in the industry to evaluate the cyber security maturity of organisations. Through these existing frameworks, organisations' current cyber security maturity level can be determined to establish a roadmap towards attaining the desired maturity level. Despite the importance of a cyber security framework against cyber-attacks for organisations [8], startups experience difficulties developing an appropriate framework for building up their cyber security maturity [11]. Without a clear framework, technology startups cannot invest properly in the suitable security measures. Poorly executed security measures result in poor cyber security, which reflects a low cyber security maturity level. Organisations can defend themselves from cyber-attacks that cause data breaches and financial losses by investing in the latest security measures [14].

A. CYBER SECURITY FRAMEWORKS

There are existing cyber security frameworks used by industry practitioners to assess cyber risks and determine the cyber security maturity posture of their organisations. Some of the commonly-used cyber security frameworks include the National Institute of Standards and Technology (NIST), International Organisation for Standardization (ISO) 27001, Control Objectives for Information and Related Technologies (COBIT 5), Cyber Security Capability Maturity Model (C2M2), Capability Maturity Model Integration (CMMI). However, these frameworks lack the end-to-end structure on

assessing cyber risks, determining the cyber security maturity levels and quantifying the returns of security investments based on the mitigation measures. Technology startups do not have the budget to invest in cyber security [7]. As such, the ability to obtain an end-to-end viewpoint on the cyber maturity posture will allow management to make proper decisions on the investment that they make to implement cyber security measures. In order to do this, the ability to assess cyber risks, determining the cyber security maturity level and quantifying the returns of security investments are necessary to be included in the end-to-end framework.

The existing cyber security frameworks are also generally used in traditional setups. The control objectives in the frameworks are broad and aplenty which take a significant amount of time (e.g., 3 to 6 months) to complete. Technology startups are known to be lean and agile, and build products with speed through innovation [41]. Thus, they do not have the luxury of time to complete a cyber security assessment which takes 3 to 6 months. As such, the control objectives in the cyber security frameworks need to be more streamlined and focused for technology startup. With a leaner framework for technology startup, this will assist in shortening the time frame to complete the cyber security assessment.

B. CYBER SECURITY MATURITY LEVELS

Cyber Security Maturity Levels help technology startups to determine their current and target maturity level [28]. It provides a good understanding for the startup to determine their existing cyber security posture and the gaps which need to be remediated in order to achieve their target maturity level. Knowing the cyber security maturity levels help cyber security practitioners to better manage the security of their organisations. According to [30], 12 cyber security maturity models have been identified between 3 to 5 maturity levels. From a maturity scale of 1 to 5, a startup with level 1 in the maturity scale has the lowest cyber security posture with very weak cyber defences which make the company susceptible to cyber-attacks. On the other hand, a startup with a 4 in the maturity scale have an above average cyber security posture with strong defences against malicious perpetrators.

The cyber security maturity level is determined by the number of effective cyber security and data protection controls implemented in the organisation. The number of effective cyber security and data protection controls is in turn determined by the amount of cyber security investments that have been allocated to mitigate cyber risks identified in the organisation. Knowing the cyber security maturity levels is important especially for technology startups as it helps management to appropriately cater cyber security investments so that they can right-size their cyber security measures depending on the current and target maturity level of the startup.

Cyber security frameworks have been extensively explored and discussed in the literature. However, end-to-end cyber security maturity assessment frameworks for SMEs, especially technology startups, have not been systematically reviewed, which is addressed in the current study. Focusing on technology startups, this study presented a comprehensive overview of the cyber security maturity assessment framework and a quantification approach to determine the return of cyber security investments. The end-to end framework will help technology startups to effectively review risks, appropriately identify the cyber security maturity level and provide management with sufficient data to make decisions in justifying investments related to cyber security. With such a framework, this will help technology startups to secure their enterprise against cyber-attacks and reduce the risk of becoming an attack vector to their clients which can be organisations such as MNCs, governments and financial institutions.

III. SYSTEMATIC LITERATURE REVIEW

The systematic literature review (SLR) can determine future research in a particular field. SLR helps researchers to obtain a firm grasp of the field of study and recognize the current research trends and gaps [16]. SLR must be comprehensively methodologically performed with rigor to eliminate bias. It should be beyond a collection of research articles; these research articles should be analytically and objectively reviewed and summarised [17]. With that, SLR was performed in this study to identify, evaluate, and summarise the findings of prior studies within a particular field of study [15].

For this study's SLR, several research questions were clearly established:

1) What cyber security maturity assessment (CSMA) frameworks are available for use in various industries?
2) Are these existing CSMA frameworks targeted for implementation in technology startups?
3) Do these existing CSMA frameworks determine the cyber security maturity level?
4) What are the shared control domains among these existing CSMA frameworks?
5) Do the existing CSMA frameworks incorporate the quantification of the return of cyber security investments?

This study gathered research articles from the following digital databases: IEEE explore (ieeexplore.ieee.org); Scopus (www.scopus.com); Springer (www.springer.com); Web of Science (http://apps.webofknowledge.com). This study targeted research articles from January 2011 to June 2022 using the following keywords: ''Cyber Security Maturity Assessment Model''; ''Cyber Security Maturity Assessment Framework''; ''Cyber Security Maturity Assessment''; ''Cyber Security Maturity Assessment'' AND ''Technology Startup''; ''Cyber Security Maturity Assessment Framework'' AND ''Technology Startup''; Cyber Security Maturity Assessment Model'' AND ''Technology Startup''; ''Cyber Security Maturity Assessment'' AND ''SME''; ''Cyber Security Maturity Assessment Framework'' AND ''SME''; ''Cyber Security Maturity Assessment Model'' AND ''SME''; ''Cyber Security Maturity Assessment'' AND ''Startup''; ''Cyber Security Maturity

TABLE 1. Inclusion and exclusion criteria.

S/N	Inclusion Criteria	Exclusion Criteria
1	Cyber security maturity assessment framework/model in technology startups	Research articles on cyber security maturity assessment framework/model with no reference to assessing cyber risks
2	Cyber security maturity assessment framework/model in startups	Research articles on cyber risk assessment framework/model with no reference to assessing cyber security maturity
3	Cyber maturity assessment framework or model for SMEs	Research articles with no reference to cyber security maturity assessment or cyber risk assessment
4	Only research articles written in English	Research articles written in languages other than English
5	Cyber security maturity assessment in various industry sectors and different organisational types	Unpublished articles, theses, references, or textbooks
6	Related research articles published between January 2011 to June 2022	Related research articles published before January 2011

Assessment Framework'' AND ''Startup''; ''Cyber Security Maturity Assessment Model'' AND ''Startup''. As SMEs and startups share similar size [5], the search included ''SME'' to cover all related small businesses.

Table 1 summarises the inclusion and exclusion criteria of this study to ensure a targeted search with respect to the research questions. All selected research articles were saved in Mendeley (www.mendeley.com), which is a reference management software that manages scholarly publications.

The PRISMA methodology, which incorporates an evidence-based minimum set of items, was employed in this study for efficient reporting of systematic reviews and meta-analyses. Figure 1 presents this study's PRISMA flowchart [18].

Based on the keywords used in the systematic literature review, this study identified 1,772 (including duplicates) research articles published in IEEE explore, Scopus, Springer, and Web of Science using the described search strings in the identification stage. There were 51 articles extracted from IEEE Explore, 175 from Scopus, 74 from Web of Science and 1472 from Springer as shown in Figure 1.

The initial screening retained a total of 620 research articles after all duplicates were removed. The screening process further excluded a total of 550 research articles according to the inclusion and exclusion criteria that have been identified as per Table 1.

The abstracts of the remaining 70 research articles were then reviewed which excluded 27 research articles. Although the excluded research articles consisted of relevant keywords in the title, abstract, and content, these research articles

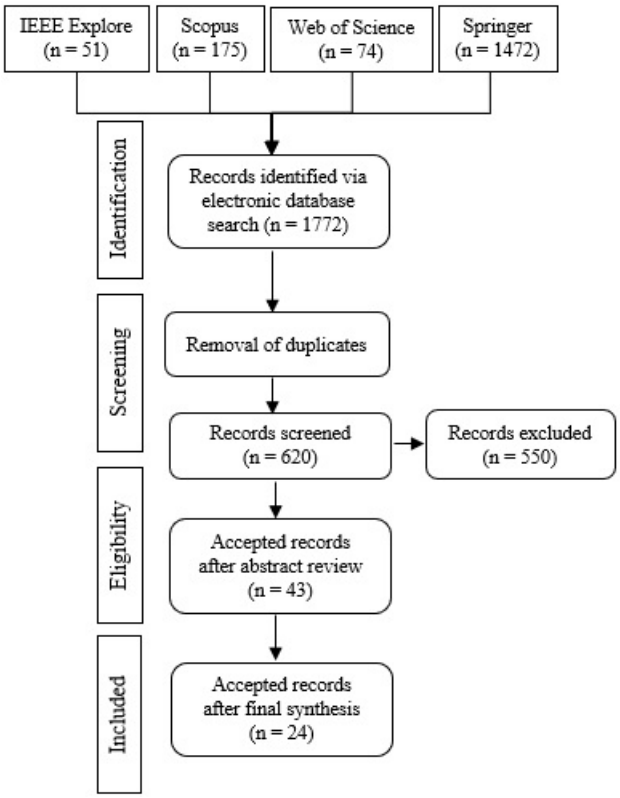

FIGURE 1. PRISMA flowchart.

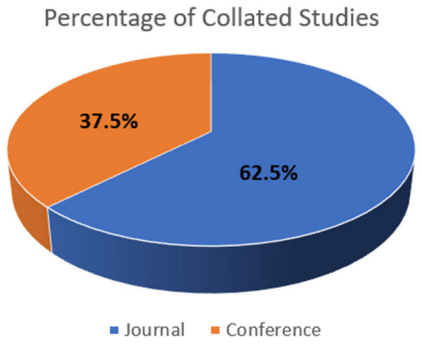

FIGURE 2. Percentage of collated studies.

focused on cyber risk with no context of cyber security maturity and vice versa. These research articles also did not address this study's research questions. After the final synthesis, 24 research articles have been accepted for an in-depth analysis.

A. OVERVIEW OF SELECTED STUDIES

24 articles were selected for this research. Among them, 9 papers appeared in conference proceedings while 13 papers were published in journals. The numbers in percentages are represented in Figure 2.

Figure 3 shows the number of papers by year of publication based on the 24 papers that have been selected in this systematic literature review. The graph indicates that there

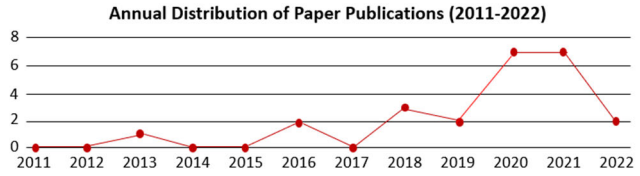

FIGURE 3. Number of papers by year of publication.

is an increase of publication from 2019 onwards. The low distribution of papers in 2022 was as of 31 Aug.

IV. THREATS TO VALIDITY

The potential biasness and the data extraction in an imprecise manner could constrain our findings and pose a major threat to how this SLR is conducted. The four common threats to validity have been taken into account: constructing validity, internal validity, external validity and conclusion validity [40]. Initially, the search terms used may not be able to extract all relevant papers in the identified databases, but manual scrutiny was conducted in the reference section of each paper to further drill down and extract the papers that fall under the research area's realm. An independent evaluation of each of the 43 papers was conducted to ensure relevance to the research area and questions. The selection of the 24 journal papers was conducted as per the PRISMA guidelines [18] to reduce the risk of missing relevant papers and ensure the selected papers can address the research questions and consider the inclusion and exclusion criteria. Several combinations of the search terms were used to avoid the accidental exclusion of relevant papers. Following the PRISMA guidelines provide reasonable assurance, without bias and using the objective criteria, the selected and reviewed papers are among the most relevant studies related to the research area and relevant to the research questions that have been determined.

V. FINDINGS

Data extraction is conducted based on the analysis of the keywords in the 24 selected papers and depicted in Figure 2 below using the VOSviewer software. The VOSviewer helped to identify the keywords which appeared most often in the articles and the links between the authors of the articles. The bigger bubbles showed the keywords which appeared most often.

This analysis is required to gather the results of the research in order to address the research questions (RQs) which have been determined for this systematic literature review. Data extraction was performed on the selected research articles (n=24), and the results are discussed with respect to this study's research questions (RQs).

RQ1: What are the cyber security maturity assessment (CSMA) frameworks available for use in various industries?

Table 2 presents the identified CSMA frameworks from all 24 research articles, which were identified as available for use in various industries across different countries. A few research articles highlighted the same CSMA framework. For instance, seven research articles [25], [28], [30], [32], [33], [35], [37] focused on the Cyber Security Capability Maturity Model (C2M2), whereas four research articles [27], [9], [33], [37] utilized the Control Objectives for Information and Related Technologies (COBIT) Framework. Several research articles also repeated and described the same framework in their literature review.

RQ2: Are these CSMA frameworks targeted for implementation in technology startups?

The analysis further revealed only one CSMA framework [28] was targeted for implementation in technology startups, which proved the lack of a CSMA framework for technology startups. In the research article entitled "Adoption of COBIT 5 Framework in Risk Management for Startup Company", a risk management model was described concerning the processes of the COBIT 5 Framework. Considering that SMEs and startups are similar in terms of size [5], seven other research articles that focused on CSMA frameworks for SMEs were also identified:

1) Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence [9]
2) The framework of Effective Risk Management in Small and Medium Enterprises (SMEs): A Literature Review [19]
3) A Dynamic Simulation Approach to Support the Evaluation of Cyber Risks and Security Investments in SMEs [22]
4) A Novel Cybersecurity Framework for Countermeasure of SMEs in Saudi Arabia [26]
5) Calculated Risk? A Cybersecurity Evaluation Tool for SMEs [29]
6) Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs [31]
7) Reference Framework "HOGO" for Cybersecurity in SMEs based on ISO27002 and 27032 [38]

Overall, this study identified 37 CSMA frameworks from 24 research articles. Adding to that, only seven frameworks were reported to be specifically targeted for SMEs, whereas only one framework for startups was identified. These results reaffirmed the need to emphasize the CSMA framework for technology startups.

RQ3: Do the existing CSMA frameworks assess the cyber security maturity level?

Table 3 presents CSMA frameworks that determine the cyber security maturity level. Assessing risk without determining the cyber security maturity level limits the ability of organisations to assess their current cyber security posture and to determine the intended or target cyber security posture. Having insights on the cyber security maturity level enables organisations to allocate the appropriate investments to enhance their cyber security maturity or posture [14].

Referring to Table 3, these frameworks were highlighted in 15 research articles. The remaining eight research articles

TABLE 2. Relevant papers describing CSMA framework.

No.	CSMA Framework	Ref
1	Committee of Sponsoring Organisations of the Treadway Commission (COSO)	[19]
2	ISO 21827	[20], [33], [35]
3	Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)	[21], [28], [32], [33], [35]
4	SMECRA (SME Cyber Risk Assessment) Methodology	[22]
5	Holistic Cybersecurity Maturity Assessment Framework (HCYMAF)	[23]
6	CyberGov (Cybersecurity Governance) Framework	[24]
7	Cyber Security Capability Maturity Model (C2M2)	[25], [28], [30], [32], [33], [35], [37]
8	Information Security Management Maturity Model (ISM3)	[25], [30], [33], [37]
9	The Publisher's Programme Overview for Information Security Management Assistance (PRISMA)	[25]
10	ISO 27002	[25], [38]
11	Holistic Cybersecurity SME's Coordination Model	[26]
12	COBIT Framework	[27], [9], [33], [37]
13	Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2)	[28], [33], [35]
14	National Initiative for Cybersecurity Education Capability Maturity Model (NICE)	[28], [30], [32], [33], [35]
15	Federal Financial Institute of Examination Council Capability Maturity Model (FFIEC-CMM)	[28], [32]
16	African Union Maturity model for Cybersecurity (AUMMCS)	[28], [32]
17	National Institute of Standards and Technology (NIST)	[9], [29], [30], [33]
18	Health Information Trust Alliance (HITRUST CSF)	[9]
19	A Pedagogic Cybersecurity Framework (PSF)	[9]
20	Centre for Internet Security (CIS)	[9]
21	Cloud Security Alliance (CSA)	[9]
22	SME Cybersecurity Evaluation Tool (CET)	[29]
23	Information Security Evaluation Maturity (ISEM) Model	[29]
24	Systems Security Engineering Capability Maturity Model (SSE-CMM)	[30]
25	ISO 27001	[30], [35], [36]
26	Information Security Maturity Model (ISM2)	[30]
27	Gartner's Information Security Awareness Maturity Model (GISMM)	[30]
28	Information Security Framework (ISF)	[30]
29	Resilience Management Model (RMM)	[30]
30	Community Cyber Security Maturity Model (CCSMM)	[30], [33]
31	Cyber Resilience Self-Assessment Tool	[31]
32	Citigroup's Information Security Evaluation Maturity model (ISEM)	[33]
33	IBM Information Security Framework	[33]
34	Saudi Cybersecurity Maturity Assessment Framework (SCMAF)	[34]
35	ISO 15408	[35]
36	ISO 27032	[38]
37	Cyber Security Governance Maturity Model (CSGMM)	[39]

emphasised risk assessment that did not specifically include the assessment of cyber security maturity level. The detailed analysis of all 23 frameworks also revealed the application of different approaches in assessing cyber security maturity levels. However, this study identified similarities in certain frameworks. For instance, the following cyber security maturity models consist of five cyber security maturity levels but the maturity levels have been defined differently [30]:

1) Information Security Evaluation Maturity Model: 1–Complacency; 2–Acknowledgment; 3–Integration; 4–Common Practice; 5–Continuous Improvement
2) Information Security Management Maturity Model: 1–Undefined; 2–Defined; 3–Managed; 4–Controlled; 5–Optimised
3) Information Security Framework: 1–Initial; 2–Basic; 3–Capable; 4–Efficiency; 5–Optimising
4) Community Cyber Security Maturity Model: 1–Initial; 2–Advanced; 3–Self-Assessed; 4–Integrated; 5–Vanguard

On the other hand, the following cyber security maturity models consist of three to four cyber security maturity levels but define cyber security maturity level differently [30]:

1) Gartner's Information Security Awareness Maturity Model: 1–Blissful Ignorance; 2–Awareness; 3–Corrective; 4–Operational Excellence
2) Resilience Management Model: 1–Incomplete; 2–Performed; 3–Managed; 4–Defined
3) Nice Cyber Security Capability Maturity Model: 1–Limited; 2–Progressing; 3–Optimised

Overall, the results demonstrated the absence of a singular CSMA framework to determine organisations' cyber security maturity level, including technology startups.

RQ4: What are the shared control domains between the existing CSMA frameworks?

Fundamentally, control domains are necessary as key controls for risk assessment. Table 4 presents the extracted shared control domains among the CSMA frameworks reported in seven research articles [20], [25], [28], [31], [32], [34], [38].

Based on the obtained results, common control domains that can be streamlined and evaluated in the risk assessment stage were found evident. These common control domains

TABLE 3. Frameworks which include CSMA.

No.	CSMA Framework	Ref
1	Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)	[21], [28], [32], [33], [35]
2	Holistic Cybersecurity Maturity Assessment Framework (HCYMAF)	[23]
3	CyberGov (Cybersecurity Governance) Framework	[24]
4	Cyber Security Capability Maturity Model (C2M2)	[25], [28], [30], [32], [33], [35], [37]
5	Information Security Management Maturity Model (ISM3)	[25], [30], [33], [37]
6	The Publisher's Programme Overview for Information Security Management Assistance (PRISMA)	[25]
7	Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2)	[28], [33], [35]
8	National Initiative for Cybersecurity Education Capability Maturity Model (NICE)	[28], [30], [31], [33], [35]
9	Federal Financial Institute of Examination Council Capability Maturity Model (FFIEC-CMM)	[28], [32]
10	African Union Maturity Model for Cybersecurity (AUMMCS)	[28], [32]
11	National Institute of Standards and Technology (NIST)	[9], [29], [30], [33]
12	SME Cybersecurity Evaluation Tool (CET)	[29]
13	Information Security Evaluation Maturity Model (ISEM)	[30]
14	Systems Security Engineering Capability Maturity Model (SSE-CMM)	[30]
15	Information Security Maturity Model (ISM2)	[30]
16	Gartner's Information Security Awareness Maturity Model (GISMM)	[30]
17	Information Security Framework (ISF)	[30]
18	Resilience Management Model (RMM)	[30]
19	Community Cyber Security Maturity Model (CCSMM)	[30], [33]
20	Cyber Resilience Self-Assessment Tool	[31]
21	Citigroup's Information Security Evaluation Maturity (ISEM) Model	[33]
22	Saudi Cybersecurity Maturity Assessment Framework (SCMAF)	[34]
23	Cyber Security Governance Maturity Model (CSGMM)	[39]

can be classified as the highest priority, which ultimately exhibit substantial risk impact on organisations. The common key control domains can be generalised as follows:

- People: This domain incorporates the organisation's human capital under the management of the Human Resource function. It consists of workforce management and the capabilities and educational qualifications of employees in key positions.
- Process: This domain covers all organisational processes from document maintenance, change and configuration management, asset management, and cybersecurity to programme management. It helps identify and manage all related security development and management processes.
- Technology: This domain focuses on the application, development, implementation, and maintenance of devices and technologies. This implements a data loss prevention tool that prevents data leakage.
- Compliance: This domain involves monitoring the organisation's compliance with information security policies, regulatory standards, and industry certifications. For instance, the organisation must comply with the ISO27001 certification.

TABLE 4. Shared control domains.

No.	Control Domains	Ref
1	Technology, Vulnerability, Risk, Impact, System, Entity, SubSystem, Capability, Threat and Process	[20]
2	Risk Management, Security Policy and Plan Management, Human Resource Management, Physical Security Management, IT Security Management, Communication Security Management, Security Technology Management, Security Event and Incident Management, Security Audit and Compliance Management	[25]
3	Asset, Change and Configuration Management, Cybersecurity Programme Management, Event and Incident Response, Continuity of Operation, Identify and Access Management, Information Sharing and Communications, Risk Management, Situational Awareness, Supply Chain and External Dependencies Management, Threat and Vulnerability Management and Workforce Management	[28], [32]
4	Risk, Assets, Access, Threat, Situation, Sharing, Response, Dependencies, Workforce and Cyber	[28], [32]
5	Asset Management, Threat and Vulnerability Management, Incident Analysis, Awareness and Training, Information Security, Detection Processes and Continuous Monitoring, Business Continuity Management, Information Sharing and Communication	[31]
6	Governance, Asset Management, Cybersecurity Risk Management, Physical Security, Third Party Security and Logical Security	[34]
7	People, Organisational Document, Process and Technology	[37]

Instead of having comprehensive control domains, this study identified five key domains which can be examined during the risk assessment stage.

RQ5: Is quantifying the return of cyber security investments embedded as part of the CSMA framework?

This study identified one research article entitled "A Dynamic Simulation Approach to Support the Evaluation of Cyber Risks and Security Investments in SMEs" [22] that highlighted its framework's capability to evaluate SMEs' cyber security investments. The study examined the targeted investments based on the risks posed and incorporated various scenarios to evaluate the cyber security investments according to several standard parameters. In one of its simulations, an organisation experiences losses due to cyber-attack, suggesting its need to allocate more investments in cyber security. As a result, the organisation's losses reduced

and eventually stabilised with increased investments in cyber security.

The lack of a quantification model embedded in an end-to-end cyber security maturity assessment framework for technology startups is a critical concern, especially when startups are highly vulnerable against the increasing rise of cyber-attacks. Technology startups cannot quantify and allocate the appropriate investments in cyber security without risk quantification.

A. GAP ANALYSIS

The existing cyber security frameworks are used by cyber security practitioners in various industries but there is a lack of a cyber security framework to assess the maturity level specifically for a technology startup from a cyber security standpoint. Out of the 37 frameworks reviewed, only seven were specifically targeted for SMEs, and only one framework was identified for technology startups. Though SMEs and startups are similar in terms of size [5], the fundamental difference is that technology startups are known for agility and thrives on innovation with information technology.

Based on the frameworks reviewed to determine the cyber security maturity levels, there are different approaches towards assessing the cyber security maturity levels. Though there are similarities in the maturity level, they are defined differently and are not suitable for a technology startup. The cyber security maturity levels for technology startups should be aligned with the stages of the startup lifecycle for clear understanding based on the investments the startup received in each stage. Figure 3 shows an appropriate cyber security maturity level based on each stage of the startup lifecycle.

Different cyber security frameworks have a variety of control domains. However, there is no framework which has control domains to assess the key controls specific for a technology startup. After analysing the control domains from the cyber security frameworks included in this study, five key domains have been extrapolated to be analysed as part of the Risk and Controls Assessment phase.

There is also a lack of a Cyber Quantification phase embedded in the cyber security framework. Since technology startups is a lean organisation, it is important to ensure that the security budget is used prudently. In order to do this, there should a cyber quantification model to calculate the return of security investments based on the mitigation costs for the control deficiencies. The return of security investments would allow management to make a proper decision when allocating the budget to invest in cyber security measures.

First and foremost, the analysis of the cyber security frameworks selected in this study have shown that there is a lack of a specific cyber security framework to examine the key control domains in a technology startup. There is no framework which assess the cyber security maturity level specifically for a technology startup. Finally, there isn't an end-to-end framework which is available to assess cyber risk, determine the cyber security maturity level and calculate the returns of cyber security investments. An end-to-end cyber security framework provides an overview to assess cyber security risk and justify mitigating measures in a more effective manner.

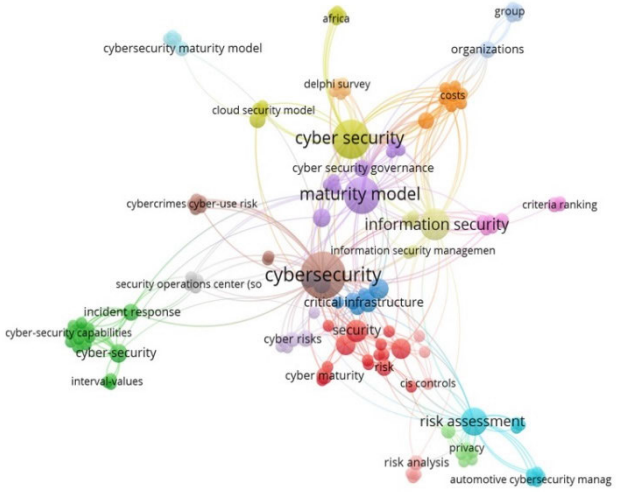

FIGURE 4. VOSviewer network visualization.

B. PROPOSED CSMA FRAMEWORK

There are existing frameworks to assess the cyber security maturity of organisations. However, the frameworks are broad and generic, and thus not specific enough to be applied in technology startups. Since startups tend to be a lean organisation with limited resources, a new framework needs to be developed which is customised and focused in identifying, mitigating and quantifying risks in a technology startup. The new Cyber Security Maturity Assessment (CSMA) framework targets specifically at technology startups and provide a holistic and end-to-end framework. The CSMA framework consists of three phases; Risk and Control Assessment, Cyber Security Maturity Level and Cyber Quantification as shown in Figure 4 below.

After extrapolating the key control domains for technology startups from the existing cyber security frameworks, the People, Process, Product, Platform and Compliance or the 4P1C domains are introduced. The 4P1C domains would allow a more streamlined approach in conducting a cyber security maturity assessment and at a much quicker pace.

In Phase 1, a Risk and Control Assessment is conducted to assess the cyber risks. Each of the 4P1C domains are broken down into several sub-domains, and each of the sub-domains may contain one or more key control objectives which need to be assessed. In the Risk and Control Assessment phase, the risk assessment rating and risk treatment are derived. Phase 2 determines the cyber security maturity level of each of the key controls, sub-domains, the 4P1C domains and the overall cyber security maturity level of the technology startup. Finally, Phase 3 calculates the return of security investment for each of the mitigating measures using an enhanced version of the Return of Security Investment (ROSI) formula [42].

The proposed CSMA framework provide an avenue to effectively assess cyber risks using the 4P1C model,

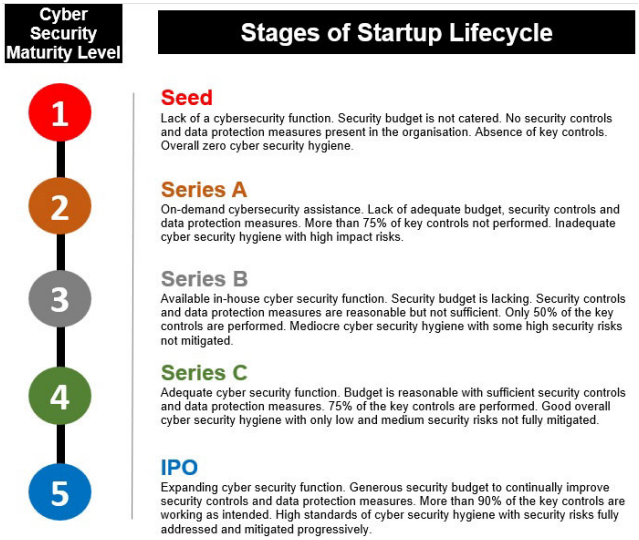

FIGURE 5. Cyber security maturity level for technology startups.

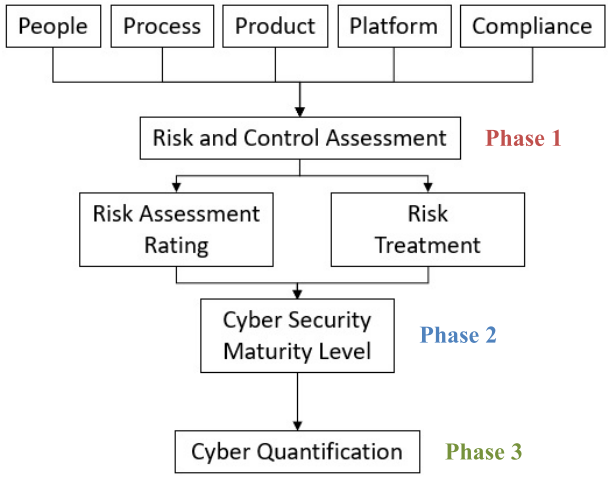

FIGURE 6. Cyber security maturity framework.

determine cyber security maturity level and quantify the returns of security investment in a technology startup. Instead of using a comprehensive framework with significant number of controls which are not applicable for a technology startup, the proposed framework can be used to assess cyber risks in a more objective, focused and streamlined manner. Determining the cyber security maturity level allow the required security controls to be implemented in order to address the identified gaps and finally quantifying the costs of mitigations and the returns of security investments provide management with sufficient data to justify the need to invest in appropriate cyber security solutions.

VI. CONCLUSION AND FUTURE WORK

Technology startups are subjected to cyber-attacks on a frequent basis [2]. The impact of cyber-attacks on smaller organisations like startups is more severe than what larger organisations experience due to their limited financial resources. It may even result in the closure of a startup. Startups with limited financial resources to properly invest in cyber security are more likely to be targeted by malicious perpetrators [6]. Startups must gain their clients' trust and confidence by withstanding against cyber-attacks and building a secure and reliable product for their clients. A cyber security maturity assessment framework can substantially benefit technology startups in evaluating their cyber risks, recognizing their current and future cyber security posture, and quantifying the return of their cyber security investments based on the mitigation costs. Such a framework enables technology startups to allocate appropriate investments in cyber security to implement the required security measures based on the identified cyber risks.

This study performed a systematic literature review on cyber security maturity assessment frameworks for technology startups. Referring to the PRISMA checklist, all five research questions were addressed through the analysis of 24 selected research articles, which revealed several key points. Firstly, there is a lack of CSMA framework specifically for technology startups. This study extracted a total of 37 CSMA frameworks from the 24 research articles. However, only seven frameworks were specifically meant for SMEs, but only one framework was targeted for startups. These results proved the need to implement a streamlined CSMA framework for technology startups. Secondly, despite the shared similarities in the cyber security maturity levels among specific frameworks, the levels were defined differently, which proved the absence of a singular framework that can assess the cyber security maturity level of technology startups. Finally, in the review of 24 selected research articles, only one highlighted the aspect of investments in cyber security for SMEs. No other research articles highlighted the quantification of the return of cyber security investments for technology startups.

From this literature review, it can be highlighted that the existing cyber security frameworks used by industry practitioners are not suitable to be implemented in an agile and lean technology startup. The cyber security maturity model in the existing frameworks is not appropriately defined to suit the different stages in the startup lifecycle. The existing frameworks are also not embedded with a cyber quantification phase which is key to calculate the return of security investments for the startup. Without an end-to-end cyber security maturity assessment framework, management in technology startups is not able to obtain relevant data in order to justify the need to invest in cyber security measures.

As this study only targeted literature from IEEE explore, Scopus, Springer, and Web of Science, other relevant publications may have been excluded from this analysis. Therefore, it is recommended for future research to also explore other repositories. Researchers can also use the proposed model for technology startups in the different industry sectors such as fintech, logistics and e-commerce. Each country has different cyber security and data protection regulations; hence the proposed framework can also be tested on technology startups in the different countries to evaluate the effectiveness

of conducting the assessment. SMEs and MNCs in different industry sectors may also want to adopt this proposed framework instead of using a broad framework with significant number of controls which take a long time and plenty of resources to complete. This framework can thus be utilised as a lightweight approach for the SMEs and MNCs to conduct the assessment.

REFERENCES

[1] Singapore Business Review, Singapore. (2022). *Singapore Cyber Attacks Soar 145% YoY in 2021*. [Online]. Available: https://sbr.com.sg/information-technology/news/singapore-cyber-attacks-soar-145-yoy-in-2021

[2] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Ephiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Comput. Secur.*, vol. 105, pp. 1–20, Mar. 2021.

[3] B. Cerin, "Cyber security risk is a board-level issue," in *Proc. 43rd Int. Conv. Inf., Commun. Electron. Technol. (MIPRO)*, Sep. 2020, pp. 384–388.

[4] C. Zuszsanna, "Startup: Hype or tendency?" *J. Org. Culture, Commun. Conflict*, vol. 24, no. 3, pp. 1–9, 2020.

[5] *Ministry of Trade and Industry*. Accessed: Jul. 20, 2022. [Online]. Available: https://www.mti.gov.sg

[6] A. L. Mitrofan, E. V. Cruceru, and A. Barbu, "Determining the main causes that lead to cybersecurity risks in SMEs," *Bus. Excellence Manage.*, vol. 10, pp. 38–48, Dec. 2020.

[7] T. Mshvidobadze, "Security issues for digital technology entrepreneurships and startups," *Sci. Practical Cyber Secur. J.*, vol. 4, no. 4, pp. 66–73, 2020.

[8] L. Sanchez, A. S. Olmo, E. F. Medina, and M. Piattini, "Security culture in small and medium-sized enterprise," *Commun. Comput. Inf. Sci.*, vol. 110, pp. 315–324, Oct. 2010.

[9] A. A. Garba and A. M. Bade, "An investigation on recent cyber security frameworks as guidelines for organizations adoption," *Int. J. Innov. Sci. Res. Technol.*, vol. 6, pp. 103–110, Feb. 2021.

[10] A. Alahmari and B. Duncan, "Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment (CyberSA)*, Jun. 2020, pp. 1–5.

[11] A. Rabii, S. Assoul, K. O. Touhami, and O. Roudies, "Information and cyber security maturity models: A systematic literature review," *Inf. Comput. Secur.*, vol. 28, no. 4, pp. 627–644, Jun. 2020.

[12] Action Community for Entrepreneurship, Singapore. (2022). *Creating a Future-Ready Startup Ecosystem*. [Online]. Available: https://ace.org.sg/wp-content/uploads/2022/01/ACE-Position-Paper-Jan-2022.pdf

[13] Ponemon Institute, Singapore. (2019). *2019 Global State of Cybersecurity in Small and Medium-Sized Businesses*. [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/security/ponemon-report-smb.pdf

[14] T. Ncubukezi, L. Mwansa, and F. Rocaries, "A review of the current cyber hygiene in small and medium-sized businesses," in *Proc. 15th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2020, pp. 1–6.

[15] Angraini, R. A. Alias, and Okfalisa, "Information security policy compliance: Systematic literature review," *Proc. Comput. Sci.*, vol. 161, pp. 1216–1224, Jan. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050919319465 and https://www.researchgate.net/scientific-contributions/Okfalisa-Okfalisa-2212519726

[16] I. Tikito and N. Souissi, "Meta-analysis of systematic literature review methods," *Int. J. Mod. Educ. Comput. Sci.*, vol. 2, pp. 17–25, Feb. 2019.

[17] C. Okoli and K. Schabram, "A guide to conducting a systematic literature review of information systems research," *Sprouts, Work. Papers Inf. Syst.*, vol. 10, no. 26, pp. 1–51, May 2010.

[18] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *Ann. Internal Med.*, vol. 89, no. 9, pp. 873–880, Sep. 2009.

[19] N. Ekwere, "Framework of effective risk management in small and medium enterprises (SMEs): A literature review," *Bina Ekonomi*, vol. 20, no. 1, pp. 23–46, Apr. 2016.

[20] R. Anass, A. Saliha, and R. Ounsa, "A concept & compliance study of security maturity models with ISO 21827," in *Proc. 22nd Int. Conf. Enterprise Inf. Syst.*, 2020, pp. 385–392.

[21] R. M. Adler, "A dynamic capability maturity model for improving cyber security," in *Proc. IEEE Int. Conf. Technol. Homeland Secur. (HST)*, Nov. 2013, pp. 230–235.

[22] S. Armenia, M. Angelini, F. Nonino, G. Palombi, and M. F. Schlitzer, "A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs," *Decis. Support Syst.*, vol. 147, Aug. 2021, Art. no. 113580.

[23] A. Aliyu, L. Maglaras, Y. He, I. Yevseyeva, E. Boiten, A. Cook, and H. Janicke, "A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom," *Appl. Sci.*, vol. 10, no. 10, p. 3660, May 2020.

[24] M. Yassine, M. Belaissaoui, and S. Abdelkebir, "A maturity framework for cybersecurity governance in organizations," *EDP Audit, Control, Secur. Newslett.*, vol. 63, no. 6, pp. 1–22, May 2021.

[25] F. Ghaffari and A. Arabsorkhi, "A new adaptive cyber-security capability maturity model," in *Proc. 9th Int. Symp. Telecommun. (IST)*, Dec. 2018, pp. 298–304.

[26] L. Ajmi, Hadeel, N. Alqahtani, A. U. Rahman, and M. Mahmud, "A novel cybersecurity framework for countermeasure of SME's in Saudi Arabia," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, May 2019, pp. 1–9.

[27] Y. Kusumaningrum, "Adoption of COBIT 5 framework in risk management for startup company," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 3, pp. 1446–1452, Apr. 2021.

[28] A. A. Garba, M. M. Siraj, and S. H. Othman, "An explanatory review on cybersecurity capability maturity models," *Adv. Sci., Technol. Eng. Syst. J.*, vol. 5, no. 4, pp. 762–769, 2020.

[29] M. Benz and D. Chatterjee, "Calculated risk? A cybersecurity evaluation tool for SMEs," *Bus. Horizons*, vol. 63, no. 4, pp. 531–540, Jul./Aug. 2020.

[30] N. T. Le and D. B. Hoang, "Can maturity models support cyber security?" in *Proc. IEEE 35th Int. Perform. Comput. Commun.*, Dec. 2016, pp. 1–7.

[31] J. F. Carias, S. Arrizabalaga, L. Labaka, and J. Hernantes, "Cyber resilience self-assessment tool (CR-SAT) for SMEs," *IEEE Access*, vol. 9, pp. 80741–80762, 2021.

[32] A. Garba, A. M. Bade, M. Yahuza, and Y. Nuhu, "Cybersecurity capability maturity models review and application domain," *Int. J. Eng. Technol.*, vol. 9, no. 3, pp. 779–784, Sep. 2020.

[33] R. Kour, R. Karim, and A. Thaduri, "Cybersecurity for railways—A maturity model," *J. Rail Rapid Transit*, vol. 234, no. 10, pp. 1–20, Oct. 2019.

[34] I. Almomani, M. Ahmed, and L. Maglaras, "Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia," *PeerJ Comput. Sci.*, vol. 7, no. 2, pp. 1–26, Sep. 2021.

[35] H. Imran, M. Salama, C. Turner, and S. Fattah, "Cybersecurity risk management frameworks in the oil and gas sector: A systematic literature review," in *Advances in Information and Communication*, vol. 2. New York, NY, USA: Springer, Mar. 2022, pp. 871–894.

[36] D. Proenca and J. Borbina, "Information security management systems—A maturity model based on ISO/IEC 27001," in *Proc. Int. Conf. Bus. Inf. Syst.*, vol. 320, Jun. 2018, pp. 102–114.

[37] M. Zammani, R. Razali, and D. Singh, "Organisational information security management maturity model," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 9, pp. 668–678, 2021.

[38] C. F. Cruzado, L. S. Rodriguez-Baca, L. G. Huanca-Lopez, and E. I. Acuna-Salinas, "Reference framework 'HOGO' for cybersecurity in SMEs based on ISO 27002 and 27032," in *Proc. 12th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Jan. 2022, pp. 35–40.

[39] S. R. Hamidi, A. A. Aziz, S. M. Shuhidan, A. A. Aziz, and M. Mokhsin, "SMEs maturity model assessment of IR4.0 digital transformation," in *Proc. Int. Conf. Kansei Eng. Emotion Res.*, in Advances in Intelligent Systems and Computing, vol. 739, Mar. 2018, pp. 721–732.

[40] X. Zhou, Y. Jin, H. Zhang, S. Li, and X. Huang, "A map of threats to validity of systematic literature reviews in software engineering," in *Proc. 23rd Asia–Pacific Softw. Eng. Conf. (APSEC)*, 2016, pp. 153–160.

[41] E. S. Rasmussen and S. Tanev, "The emergence of the lean global startup as a new type of firm," *Technol. Innov. Manage. Rev.*, vol. 5, no. 11, pp. 12–19, Nov. 2015.

[42] T. Yaqoob, A. Arshad, H. Abbas, M. F. Amjad, and N. Shafqat, "Framework for calculating return on security investment (ROSI) for security-oriented organizations," *Future Gener. Comput. Syst.*, vol. 95, pp. 754–763, Jun. 2019.

MOHAMED NOORDIN YUSUFF MARICAN received the master's degree (Hons.) in internet security management from the Curtin University of Technology, Australia. He is currently pursuing the Ph.D. degree in computer science with Universiti Teknologi Malaysia. He is also an Adjunct Lecturer in cyber security with universities in Singapore, Australia, and U.K. In August 2022, he was a cyber security professional for more than 20 years working in various sectors of the industry, such as government, banking, oil and gas, consulting, social enterprise, and technology startups. He is also a member of the Information Systems Audit and Control Association (ISACA), International Information System Security Certification Consortium (ISC2), and Association of Certified Fraud Examiners (ACFE). He also holds industry certifications, such as Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Certified Fraud Examiner (CFE), and PRINCE2 Foundation and Practitioner.

SHUKOR ABD RAZAK (Senior Member, IEEE) is currently a Professor at Universiti Teknologi Malaysia (UTM) and currently seconded as the Deputy Vice Chancellor of Universiti Sultan Zainal Abidin (UNISZA), Terengganu, Malaysia. He also actively conducts several types of research in digital forensic investigation, wireless sensor networks, and cloud computing. He is the author or coauthor for many journals and conference proceedings at national and international levels. His research interests include the security issues for mobile *ad-hoc* networks, mobile IPv6, vehicular *ad-hoc* networks, and network security.

ALI SELAMAT (Member, IEEE) has been the Dean of the Malaysia Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia (UTM), Malaysia, since 2018. An academic institution established under the cooperation of the Japanese International Cooperation Agency (JICA) and the Ministry of Education Malaysia (MOE) to provide the Japanese Style of Education in Malaysia. He is currently a Full Professor with UTM, where he is also a Professor with the Software Engineering Department, Faculty of Computing. He has published more than 60 IF research papers. His H-index is 20 and his number of citations in WoS is more than 800. His research interests include software engineering, software process improvement, software agents, web engineering, information retrievals, pattern recognition, genetic algorithms, neural networks, soft computing, computational collective intelligence, strategic management, key performance indicator, and knowledge management. He is on the Editorial Board of the *Journal Knowledge-Based Systems* (Elsevier). He has been serving as the Chair for the IEEE Computer Society Malaysia, since 2018.

SITI HAJAR OTHMAN (Member, IEEE) received the Ph.D. degree from the University of Wollongong, Australia. She is currently a Senior Lecturer with the Department of Computer Science, Universiti Teknologi Malaysia (UTM). Her current research interests include cybersecurity, security management, computer forensic, conceptual modeling, disaster management, disaster recovery, and business continuity planning.