INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 16, Issue 7, (2026) E-ISSN: 2222-6990

Securing the Digital Frontier by Integrating Cybersecurity into Internal Audit Practices: A Systematic Literature Review and Future Research Agenda

Kennardi Tanujaya*
Graduate School of Business, Universiti Sains Malaysia, Penang, Malaysia and Faculty of Business and Management, Universitas Internasional Batam, Batam, Indonesia
Email: kennardi.tanujaya@uib.ac.id

Teoh Ai Ping*
Graduate School of Business, Universiti Sains Malaysia, Penang, Malaysia
*Corresponding Author Email: apteoh@usm.my

Mardianto
Faculty of Business and Management, Universitas Internasional Batam, Batam, Indonesia

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v16-i7/28711

Published Date: 29 July 2026

Abstract

In today's the increasing use of digital technologies among companies has emphasized the importance and role of cybersecurity as a new risk management dimension. Internal audit function as third line defence in preventing cyber-attack become important role to provide assurance to the organization's cybersecurity. The aim of this systematic literature review (SRL) is to identify the relationship between internal audit and cyber security and develop cybersecurity framework to ensure cyber security risk assessment performed well by internal audit. The systematic literature review utilized the ROSES (RepOrting Standards for Systematics Evidence Syntheses) publication standard and encompassed several research methodologies. Scopus, a highly significant scientific database, was utilized for the article selection in this study. The review only considered articles that were published from 2010 to 2024. The focus of the article primarily was on internal audit and cyber security. This review identified four main themes: internal audit characteristics, internal audit role, information technology and management action. An additional twelve sub-themes were derived from the four main themes. This paper systematically reviewed literature related to the internal audit and cyber security. The findings allow the companies to better understand the importance of cyber security that requires the need for internal audit function to assist the organisations in

evaluating the effectiveness and adequacy of controls to mitigate the impact of cyber security risks.
Keywords: Cybersecurity, Internal Audit, Systematic Literature Review

Introduction

Information technology (IT) is quickly being incorporated into different sectors, especially finance. While IT systems facilitate efficient and competitive everyday operations, their implementation also exposes enterprises and companies to the vulnerability of cyberattacks, including data theft, software corruption, and disruption of corporate operations. The Institute of Internal Auditors (IIA) has introduced the Three Lines Model, which has demonstrated its effectiveness in reducing cybersecurity risks by involving the first and second lines of defence (IIA, 2020). However, there is still uncertainty over the precise function of internal auditors as the third line of defence in deterring cyberattacks, and additional clarification is needed. Internal auditing has a crucial role to play in the cybersecurity assurance process (Kahyaoglu and Caliyurt, 2018). The internal audit plays a crucial role in assisting firms in effectively managing cyber threats. This is achieved through conducting an impartial evaluation of current and required controls, as well as aiding the audit committee and board in comprehending and mitigating the many risks associated with the digital realm (Delloite, 2017). Internal audit and cybersecurity are critical components of organizational risk management. As cyber threats evolve, the role of internal audit in evaluating and improving cybersecurity measures becomes increasingly important. Therefore, this review would like to explore the significance internal auditor role whether able fulfil the role as third line defence for company in cyber security. To fill the research gap, this paper aims to synthesize existing research on the intersection of these two fields between internal audit and cybersecurity, providing insights into best practices, framework, and emerging trends through SRL.

Although several SRL studies have made efforts to comprehensively examine the topic of cybersecurity, previous studies have not specifically concentrated on the role of internal audit in cybersecurity. Prior research has focused on narrow areas such as blockchain cybersecurity (Taylor *et al.*, 2020), information security awareness (Kannelønning and Katsikas, 2023; Rahim *et al.*, 2015; Rohan *et al.*, 2023) and cybersecurity incidents (Patterson, Nurse and Franqueira, 2023). To the author's knowledge, this is the first study to describe the literature review that focus of relationship between internal audit and cyber security.

The review intends to address the following research questions: What factor in internal audit influence cyber security assessment? How can these factors be addressed and developed as framework to improve cyber security assessment by internal audit? This study aims to review previous studies to fill the research gap and understand the impacts of internal audit function on cyber security assessment. The finding will help developing internal audit function with appropriate understanding to able performed their assurance to the cyber security. The next section will further explain the methodology used in this research to address the research questions

Methodology

This section explains how to obtain articles on that discuss internal audit and cyber security. The researchers applied the RepOrting Standards for Systematic Evidence Syntheses (ROSES)

review met approach, which includes the review protocol used to conduct the systematic review, formulation of research questions, systematic searching strategies, quality appraisal, and data abstraction analysis.

The Review Protocol – ROSES

Establishing publishing criteria is typically essential in providing researchers with the requisite information to evaluate and examine the quality of a review. This SRL study is based on ROSES, review methodology to doing literature review, as outlined by Haddaway *et al.* (2018). According to ROSES's founders Haddaway *et al.* (2018), ROSES may be used for a systematic review that provide comprehensive and explicit guidelines, accompanied by illustrative examples, for each step of the review procedure. including planning, conduct and reporting that able to accommodate quantitative studies and qualitative research. Firstly, this SRL created the research questions based on the protocol. Then, we adopted a systematic searching strategy to find the relevant articles that consists three primary steps: keyword identification, article screening and eligibility. Then, for the quality evaluation step to ensure the strategy and analysis of selected articles were carried out properly. Finally, we outlined data abstraction and analysis step used an integrative review approach.

Formulation of Research Questions

This study utilised the PICo (Population, Interest and Context), a tool designed to aid authors in formulating appropriate research questions for their reviews. PICo is composed of 3 main criteria: Population or Problem (P), Interest (I) and Context (C) (Lockwood, Munn and Porritt, 2015). Based on the PICo framework, the study has included 3 criteria in the review, "How does the internal audit influence the cyber security assessment?" (Problem), "cyber security assessment" (Interest) and "business organisations" (Context) which led to the formulation of the main research question – RQ1: Does the internal audit influence cyber security assessment of business organisations? RQ2: How can the internal auditor be addressed to improve cybersecurity practices within organizations?

Systematic Searching Strategies

This study use systematic searching process flow diagram according to Shaffril *et al.* (2021) (See Figure 1). There are three primary steps in systematic searching strategies: identification, screening and eligibility.

Identification

Scopus is the database that chosen because Scopus is the most effective search engine and search result can be sorted by the number of citations which makes it very useful to decide which articles are of interest (Tober, 2011). The reason for its selection is because Scopus is a biggest abstract and citation database that includes papers that have been subjected to peer review and also covers a wide range of research interest, including agriculture, biology and social science (Shaffril, Samah and Samsuddin, 2021). This study use "Title/Abstract/Keywords" to narrow down the scope and able to get the relevant articles. An identification technique has been done to search for synonyms of the study's keywords, namely related terms and variations of the primary keywords "internal audit" and "cyber security". The objective is to gather a diverse range of pertinent articles for this study by utilising a wide range of keywords for the database search. The identification method for the study topic involved reviewing synonyms of keywords from online thesauri and dictionaries,

keywords gathered from previous studies, as well as keywords recommended by Scopus and experts. As a result, the basic keyword of cybersecurity has been expanded to include additional keywords like “information security”, “information system security”, “information technology security”, “internet of things security”, “digital security”, “cloud security”, “technology security”, “internet security” and “web security”. Furthermore, the additional keywords of internal audit encompassed “internal auditing”, “audit” and "auditor”. These terms were searched in Scopus through full search string including code functions “TITLE-ABS-KEY” and Boolean operators “OR” and “AND” as conjunction to combine each keyword in SRL, as indicated in Table 1. Based on the search attempts, a total of 1,450 articles from Scopus that was discovered.

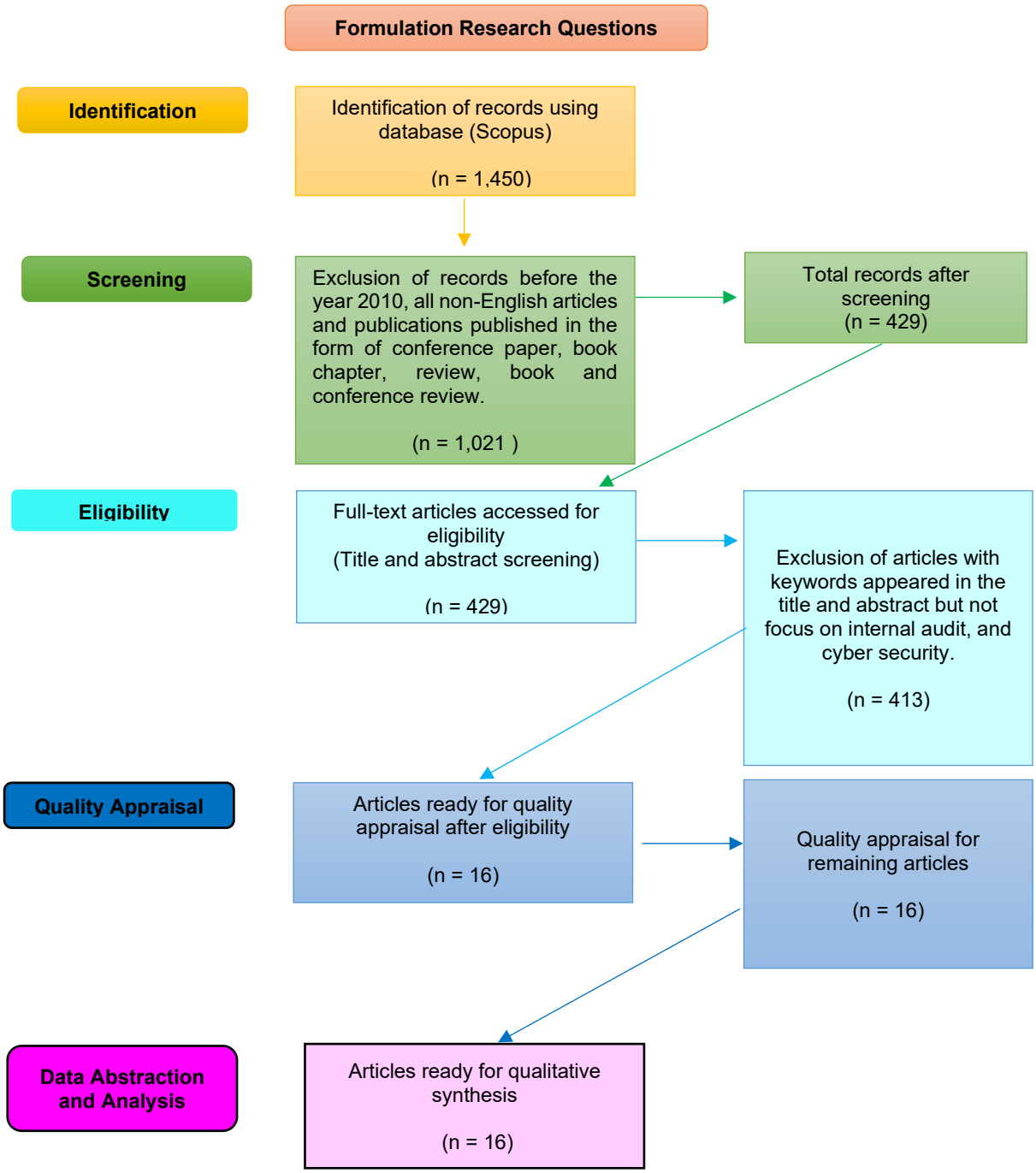

Figure 1. The flow diagram of articles selection

Source(s): Adapted from Shaffril *et al.* (2021)

Table 1
Search string used in the selected database

Database	Search String
Scopus	TITLE-ABS-KEY ((“cybersecurity” OR "cyber security" OR "information security" OR "information system security" OR "information technology security" OR "internet of things security" OR "digital security" OR "cloud security" OR "technology security" OR "internet security" OR "web security" AND "internal audit" OR "internal auditing" OR "audit" OR "auditor"))

Source: Author’s own creation

Screening

The second stage is screening process to review 1,450 articles by defining inclusion and exclusion criteria in order to select the relevant studies for SRL. The inclusion and exclusion criteria were defined to the experience of Kitchenham *et al.* (2009) that shown in Table 2. Kraus *et al.* (2020) mention that the author’s capacity to review article is important to determine the quality of literature review. In order to achieve that objectives, this SRL need to determine time frame for conducting the review (Okoli, 2015). Although research on internal audit towards cyber security on started to increase in 2018, certain related articles were published prior to that time. Hence, the time frame between 2010 and 2024 was selected for this SRL. Next, this review only includes papers for inclusion criteria and does not include conference paper, book chapters, review articles and books for exclusion criteria. According to Podsakoff *et al.* (2005), peer-reviewed journal publications undergo academic review, which enhances their credibility and makes them more commonly acknowledged as a source of higher quality. The last inclusion criterion was language, specifically limiting the study to articles written in English to prevent confusion. 1,021 articles were excluded for not meeting the inclusion and exclusion criteria for further consideration.

Table 2
Criteria of inclusion and exclusion

Criteria	Inclusion	Exclusion
Timeline	2010-2024	Earlier than 2010
Article type	Journal	Conference Proceeding, Book chapter, review article, short survey, book, etc
Language	English	Non-english

Source (s): Authors’ creation

Eligibility

Next step is eligibility process to evaluate the remaining articles. The authors read manually the titles and abstracts of each paper that suitable for full review. 413 articles were eliminated as a consequence of the abstract screening procedures. The articles were excluded for full review because it did not mention internal audit and cyber security themes. There was a total of 16 articles selected for the quality appraisal.

Quality Appraisal

In order to ensure the quality of the articles, the authors used Mixed Method Appraisal Tool (MMAT) to assess the articles developed by Hong *et al.* (2018). The research criteria evaluated articles' quality, focusing on research questions, qualitative data collection, and coherence of sources. MMAT supported these criteria, ensuring strong methodology and thorough examination of chosen qualitative sources. The authors assessed the quantitative research design based on the relevance of the sampling approach to the research objectives, including the suitability of measurement, analysis, and sample for the population. They used MMAT to integrate qualitative and quantitative data, resolve divergence and differences between research designs, and justify adopting mixed-method research to address research questions. The authors employed the Mixed Methods Appraisal Tool (MMAT) to evaluate the publications, specifically examining the coherence in the sample and analysis methods, such as random sampling versus inferential analysis. The criteria utilised for adapting the criteria established by Shaffril *et al.* (2021) to evaluate the thoroughness of the approach and analysis employed in the chosen studies are presented in Table 3.

The evaluation of each article was based on five criteria, and there were two alternatives available for displaying the results. Only articles that met a minimum of three criteria were taken into account for the subsequent stage. All differences were swiftly resolved through discussion among the researchers, and all evaluation decisions were universally agreed upon. According to this process, all authors unanimously concluded that each selected article matched the criteria for methodology and analysis. Table 4 presents a concise overview of the outcomes of the quality appraisal. Overall, a total of 16 articles fulfilled all of the specified criteria, while four items met a minimum of four criteria.

Table 3
Criteria assess the rigor of the methodology

Criteria		
Qualitative	1	Is the qualitative approach able to answer the research question?
	23	Are the data collection method able to address the research question?
	4	Are the findings sufficiently obtained from the data?
	5	Are the results sufficiently supported by the data?
	1	Is there consistency between qualitative data, sources, analysis and interpretation?
Quantitative	2	Is there a relevant sampling strategy to address the research question?
	3	Does the sample represent the target population?
	4	Are the measurements accurate?
	5	Is the risk of non-response bias low?
		Is there an appropriate statistical analysis to answer the research question?

Source (s): Authors' creation

Table 4
Results of the quality assessment

No.	Author	Methodology	Q1	Q2	Q3	Q4	Q5	Quantity fulfilled	Inclusion for review
1	Wallace *et al.* (2011)	Quantitative	/	/	/	X	/	4/5	Y
2	Steinbart *et al.* (2012)	Qualitative	/	/	/	/	/	5/5	Y
3	Steinbart *et al.* (2013)	Quantitative	/	X	/	/	/	4/5	Y
4	Steinbart *et al.* (2016)	Qualitative	/	/	/	X	/	4/5	Y
5	Islam *et al.* (2018)	Quantitative	/	/	/	/	/	5/5	Y
6	Steinbart *et al.* (2018)	Quantitative	/	/	/	/	/	5/5	Y
7	Stafford *et al.* (2018)	Qualitative	/	/	/	/	/	5/5	Y
8	Rodgers *et al.* (2019)	Quantitative	/	/	/	/	/	5/5	Y
9	Lois *et al.* (2020)	Quantitative	/	/	/	/	/	5/5	Y
10	Betti and Sarens (2020)	Quantitative	/	/	/	/	/	5/5	Y
11	Lois *et al.* (2021)	Quantitative	/	/	/	/	/	5/5	Y
12	Betti *et al.* (2021)	Quantitative	/	/	/	/	/	5/5	Y
13	Slapničar *et al.* (2022)	Quantitative	/	/	/	/	/	5/5	Y
14	Gunawan *et al.* (2023)	Qualitative	X	/	/	/	/	4/5	Y
15	Elmaasrawy and Tawfik (2024)	Quantitative	/	/	/	/	/	5/5	Y
16	Wu *et al.* (2024)	Quantitative	/	/	/	/	/	5/5	Y

Source (s): Authors' creation

Data abstraction and analysis

The selected articles were analysed for determined themes and sub-themes by looking at the abstracts and entire discussion of the publications with integrative review approach. Multiple studies (quantitative and qualitative) used in the SRL. To address the research questions, the data abstraction process involved extracting the relevant information from the reviewed studies and organizing it in tables. The study utilised the methodologies suggested by Kiger *et al.* (2021) to establish the thematic synthesis. Prior to doing their analysis, the researchers acquainted themselves with the dataset. This served as the basis for later phases. Subsequently, they meticulously encoded the data, collecting essential information from specifically chosen articles. Next, themes were derived by identifying parallels and linkages within the coded data. The synthesis was grounded in these themes and their connection to the original data (Braun and Clarke, 2019). We used Microsoft Excel and Word to record the abstracted data, grouping it into four main themes. The method was then used repeatedly for each topic to identify any potential sub-themes, resulting in twelve subthemes. After that, the authors validate the identified themes and subthemes. Following this process, it was decided to retain all four themes and twelve subthemes.

Results

Background of the selected articles

From the reviewed articles, a total of two articles conducted their studies in Greece (Lois *et al.*, 2020; Lois *et al.*, 2021) and five articles were conducted worldwide (Wallace *et al.*, 2011; Steinbart *et al.*, 2018; Islam *et al.* 2018; Slapničar *et al.*, 2022; Elmaasrawy and Tawfik, 2024). Meanwhile, Betti *et al.* (2021) conducted the research United States America, Betti and Sarens (2020) in Belgium, Rodgers *et al.* (2019) in Saudi Arabia and Wu *et al.* (2024) in Taiwan. However, study from Steinbart *et al.* (2012), Steinbart *et al.* (2013), Stafford *et al.* (2018), Steinbart *et al.* (2016) and Gunawan *et al.* (2023) do not reveal the population in their study. Table 5 explains the countries where the selected research was conducted. In relation to the research method, twelve articles focused on quantitative analysis (Wallace *et al.*, 2011; Steinbart *et al.*, 2013; Steinbart *et al.*, 2016; Islam *et al.*, 2018; Steinbart *et al.*, 2018; Rodgers *et al.*, 2019; Lois *et al.*, 2020; Lois *et al.*, 2021; Slapničar *et al.*, 2022; Gunawan *et al.*, 2023; Elmaasrawy and Tawfik, 2024; Wu *et al.*, 2024), meanwhile four articles were conducted using qualitative approach (Steinbart *et al.*, 2012; Stafford *et al.*, 2018; Betti and Sarens, 2020; Betti *et al.*, 2021). Table 6 explain the research methodology of selected studies.

With regards to publication year, one article was published in 2011 (Wallace *et al.*, 2011). Steinbart (2012, 2013 and 2016) published three articles. Three articles (Islam *et al.*, 2018; Steinbart *et al.*, 2018, Stafford *et al.*,2018) published in 2018. One article (Rodgers *et al.*, 2019) published in 2019. Both 2020 (Betti and Sarens, 2020, Lois *et al.*, 2020) and 2021 (Betti *et al.* 2021, Lois *et al.*, 2021), published two articles. One article (Slapničar *et al.*, 2022) published in 2022, one article (Gunawan *et al.*, 2023) published in 2023 and lastly two articles (Elmaasrawy and Tawfik, 2024, Wu *et al.*, 2024) published in 2024. Table 7 shows the publication years of selected studies.

Table 8 shows selected articles and their publications. Three journal were published by Managerial Auditing Journal (Islam *et al.*, 2018; Stafford *et al.*, 2018; Betti *et al.*, 2021) the three journals published by Journal of Information Systems (Steinbart *et al.*, 2013; Steinbart *et al.*, 2016; Wallace *et al.*, 2011), one was by Accounting, Organizations and Society (Steinbart *et al.*, 2018), one was by Journal of Science and Technology Policy Management (Elmaasrawy and Tawfik, 2024), three were by International Journal of Accounting Information (Steinbart *et al.*, 2012; Slapničar *et al.*, 2022; Wu *et al.*, 2024). In addition, each of the articles was by International Journal of Managerial and Financial Accounting (Lois *et al.*, 2021), International Journal of Data and Network Science (Rodgers *et al.*, 2019), Journal of World Business (Rodgers *et al.*, 2019) and Journal of Accounting and Organizational Change (Betti and Sarens, 2020).

Table 5
Countries where the selected studies were conducted

No.	Country	Articles	Count(s)
1	United States America	Betti *et al.* (2021)	1
2	Belgium	Betti and Sarens (2020)	1
3	Greece	Lois *et al.* (2020), Lois *et al.* (2021)	2
4	Saudi Arabia	Rodgers *et al.* (2019)	1
5	Taiwan	Wu *et al.* (2024)	1
6	Worldwide	Wallace *et al.* (2011), Steinbart *et al.* (2018), Islam *et al.* (2018), Slapničar *et al.* (2022), Elmaasrawy and Tawfik (2024)	5
7	Unknown	Steinbart *et al.* (2012), Steinbart *et al.* (2013), Stafford *et al.* (2018), Steinbart *et al.* (2016), Gunawan *et al.* (2023)	5

Source (s): Authors' creation

Table 6
Research design of selected articles

No.	Method	Articles	Count(s)
1	Quantitative	Wallace *et al.* (2011), Steinbart *et al.* (2013), Steinbart *et al.* (2016), Islam *et al.* (2018), Steinbart *et al.* (2018), Rodgers *et al.* (2019), Lois *et al.* (2020), Lois *et al.* (2021), Slapničar *et al.* (2022), Gunawan *et al.* (2023), Elmaasrawy and Tawfik (2024), Wu *et al.* (2024)	12
2	Qualitative	Steinbart *et al.* (2012), Stafford *et al.* (2018), Betti and Sarens (2020), Betti *et al.* (2021)	4

Source (s): Authors' creation

Table 7
Publication years of selected studies

No.	Year	Articles	Count(s)
1	2011	Wallace *et al.* (2011)	1
2	2012	Steinbart *et al.* (2012)	1
3	2013	Steinbart *et al.* (2013)	1
4	2016	Steinbart *et al.* (2016)	1
5	2018	Islam *et al.* (2018); Steinbart *et al.* (2018), Stafford *et al.* (2018)	3
6	2019	Rodgers *et al.* (2019)	1
7	2020	Betti and Sarens (2020) ; Lois *et al.* (2020)	2
8	2021	Betti *et al.* (2021); Lois *et al.* (2021)	2
9	2022	Slapničar *et al.* (2022)	1
10	2023	Gunawan *et al.* (2023)	1
11	2024	Elmaasrawy and Tawfik (2024); Wu *et al.* (2024)	2

Source (s): Authors' creation

Table 8
Selected journal and their publications

No.	Journal	Indexed	Article(s)	Count (s)
1	Managerial Auditing Journal	Q1	Islam *et al.* (2018), Stafford *et al.* (2018), Betti *et al.* (2021)	3
2	Journal of Information Systems	Q2	Steinbart *et al.* (2013), Steinbart *et al.* (2016), Wallace *et al.* (2011)	3
3	Accounting, Organizations and Society	Q1	Steinbart *et al.* (2018)	1
4	Journal of Science and Technology Policy Management	Q2	Elmaasrawy and Tawfik (2024)	1
5	International Journal of Accounting Information Systems	Q1	Steinbart *et al.* (2012), Slapničar *et al.* (2022), Wu *et al.* (2024)	3
6	International Journal of Managerial and Financial Accounting	Q3	Lois *et al.* (2021)	1
7	EuroMed Journal of Business	Q1	Lois *et al.*, (2020)	1
8	International Journal of Data and Network Science	Q2	Gunawan *et al.* (2023)	
9	Journal of World Business	Q1	Rodgers *et al.* (2019)	1
10	Journal of Accounting and Organizational Change	Q1	Betti and Sarens (2020)	1

Source (s): Authors' creation

The Developed Themes

Thematic analysis is a systematic approach used to identify, analyse, and evaluate patterns of significance or themes. This research involved analysing chosen papers to uncover patterns and important topics within the literature. It involved a careful review of each 16 articles, 4 main themes (internal audit characteristics, internal audit role, information technology and management action) and 12 sub-themes were derived by grouping related codes together, allowing for the identification of overarching patterns and recurring topics across all selected articles. The 4 themes and 12 sub-themes to address the study topic are listed in Table 9.

Table 9
The developed themes

No	Themes	Sub-themes	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Internal audit characteristics	IT knowledge		X	X		X					X				X		X
		Perception role		X	X	X												X
		IT audit competencies			X										X	X		X
		Security standards	X					X	X	X			X					
2	Internal audit role	Assurance role			X		X					X	X	X			X	X
		Advisory role					X		X						X		X	X
		Enterprise risk management																
3	Information Technology	IT relationship quality			X			X										X
		IT governance process									X	X		X				X
		Technology Audit																
4	Management action	Provide training	X								X		X					
		Top management support		X			X	X								X		

Note (s): A= Wallace *et al.* (2011), B=Steinbart *et al.* (2012), C=Steinbart *et al.* (2013), D=Steinbart *et al.* (2016), E=Islam *et al.* (2018), F=Steinbart *et al.* (2018), G=Stafford *et al.* (2018), H=Rodgers *et al.* (2019), I=Lois *et al.* (2020), J=Betti and Sarens (2020), K=Lois *et al.* (2021), L=Betti *et al.* (2021), M=Slapničar *et al.* (2022), N=Gunawan *et al.* (2023), O=Elmaasrawy and Tawfik (2024), P= Wu *et al.* (2024)
Source (s): Authors' creation

Internal Audit Characteristics

The first sub-theme under internal audit characteristics is IT knowledge. Internal auditors with detailed technical expertise in information security can establish deeper relationships with the information systems security function, while those lacking such knowledge may experience less development in their relationships (Steinbart *et al.*, 2012). Individuals responsible for assessing cybersecurity must have knowledge of information system audit techniques and security standards (Gunawan *et al.*, 2023). Steinbart *et al.* (2013) proved that the importance of auditors to possess sufficient knowledge about IT and cyber security. It would be beneficial to dedicate a significant amount of internal audit training resources to enhance the staff's IT skills, particularly in areas pertaining to information security. Hence, the internal audit able to perform effective in cyber security assessment. The knowledgeable

auditor largely will bring a greater focus on cybersecurity issues in audits. Betti and Sarens (2020) explains that as digitalization continues, internal auditors must possess adequate digital knowledge to effectively audit and mitigate risks in digitalized business processes, understanding the entire process and the implications of new technologies' use. The Internal Audit Function (IAF) and IT function quality to improve the general control of information security within organizations is significantly influenced by IT knowledge (Steinbart *et al.*, 2013; Wu *et al.*, 2024). The aspect for knowledge can be proven also through certification hold by the internal auditors. According to Islam *et al.* (2018), the specialized certifications of that internal auditor tend to be indicative of increased professional experience and knowledge to able perform effective cyber security assessment.

The next sub-theme developed under the main theme of internal audit characteristics is perception role. When the internal audit perceived its position as that of an advisor rather than an enforcer, it is more probable that a sense of mutual trust will develop between the internal audit and information systems security functions. As the level of trust between the two parties grows, their cooperation also increases (Steinbart *et al.*, 2012; 2013). Steinbart *et al.* (2016) created an instrument called SECURQUAL to assess individuals' perceptions of an organization's information security processes. The study demonstrated that SECURQUAL is a strong indicator of real security results, indicating that it could be a valuable substitute measure for these outcomes. Internal auditors' responsibilities are influenced by a company's decision-making processes, and understanding regulatory compliance requirements and their role in improving operational efficiency through effective cyber security control assessments is crucial. The board of directors and management should broaden the range of tasks assigned to IAF, promoting continuous improvement in understanding their roles, scope of work, and job responsibilities (Wu *et al.*, 2024).

Another sub-theme developed under the main theme of internal audit characteristics is IT audit competencies. The IAF's IT audit competencies are linked upon the audit's depth and scope (Héroux and Fortin, 2013). IT audit competencies exhibit a significantly positive relationship with IT governance processes, properly structured IT governance processes demonstrate a positive association with the effectiveness of security controls (Wu *et al.*, 2024). Internal audit that frequently conduct the audit risk assessment on cyber security able to enhance the information security effectiveness (Steinbart *et al.*, 2013). Risk assessment is a crucial process to identify and manage risks, with cybersecurity being a significant component of audit risk assessment. Cybersecurity risks are mandatory in information technology, and risk assessment has been proven to positively impact security and cybersecurity audits, making it a crucial component of overall risk management (Gunawan *et al.*, 2023). The internal auditor with high IT competencies able to perform high cyber security audit effectiveness to contributes better cyber security risk management (Slapničar *et al.*, 2022)

Another internal audit characteristic sub-theme that has been established is security standards. Organizations may select one or more security standards to serve as a framework for best practices and an approach to information security. These standards can be employed by internal audit during a cyber security assessment (Steinbart *et al.*, 2018). The existence of security standard on the part of internal auditors are crucial, as they will contribute to the development of security strategy aimed at reducing the incidence of violations (Lois *et al.*,

2021). Hence, compliance of security standards become important aspect that need aware by the management. The information security management is a complex task and if governed effectively, helps organizations to not only achieve security standards compliance but also maintain that compliance (Wallace, Lin and Cefaratti, 2011). Auditors can easily identify and audit user compliance with corporate security standards by expanding their internal controls investigation. They can determine if users are solely relying on existing security controls or engaging in pro-security behaviour to support corporate standards, thereby expanding their understanding of user behaviour (Stafford, Deitz and Li, 2018). Rodgers *et al.* (2019) reveals that foreignness, specifically linguistic and relational social capital, influences internal auditors' compliance with standards, potentially impacting cybersecurity controls. To mitigate emerging risks, auditors must ensure management implements preventive and detective controls, and understand the influence of linguistic and social capital on their audit approach to assess cybersecurity risk and management's response capabilities.

Internal Audit Role

Assurance role is the first sub-theme under the theme of internal audit role. Internal audit has important role to form an effective cybersecurity risk management program in order to give assurance on the security risk management (Islam *et al.*, 2018). Internal auditors must acknowledge that their role may be impacted by the company's decision-making style and processes. The board of directors and management must fully understand both the regulatory compliance requirements of the IAFs and its vital role in improving operational efficiency through efficient internal control reviews and report any deficiency regarding information security (Wu *et al.*, 2024). Thus, internal audit can add value to business firms by providing objective assurance and role regarding the effectiveness of current technical measures to confront cyber security risks and the effectiveness of contingency plans to deal with any cyber breach and the extent to which cyber risks resulting from security vulnerabilities are updated and monitored (Elmaasrawy and Tawfik, 2024).

Advisory role is the second sub-theme. Steinbart *et al.* (2013) found that internal audit's advisory role was to provide advice and guidance than when they considered the auditor to be merely a compliance monitor. The advent of digitalisation has led top management to demand internal audit departments to function increasingly as business partners rather than mere controllers. The demand for consulting activities seems to be growing in the evolving digitalised company landscape. The findings by Betti and Sarens (2020) indicate that an IAF engaging in a greater number of consulting activities might be seen as more advantageous and can encourage senior management to alter the organisational direction. Elmaasrawy and Tawfik (2024) discovered that competent internal auditors can contribute to improving cyber security by fulfilling their function as confirmatory and advisory agents, particularly in relation to proactive measures including human factors. Internal auditors could also offer guidance and insight on cybersecurity programs and risk prevention, thereby engaging in additional consulting activities. Consequently, the company anticipate the transition to a more consultative role for internal auditors will be facilitated by digitalisation. Consequently, we assert that the demand for consulting services will rise in tandem with the organization's degree of digitalisation (Betti, Sarens and Poncin, 2021). Modern internal auditors acknowledge that they must play both assurance and advisory role to improve the cyber security audit process (Wu *et al.*, 2024) and expected lead to reduction in incidence of violations (Lois *et al.*, 2021).

Enterprise risk management is the third sub-theme. Internal audits have given tasked in ERM of an organization. Internal audit function is an essential component in the overall risk management in its capacity of the third line of defence (Slapničar *et al.*, 2022). Islam *et al.* (2018) found that IAF tasked with ERM either focuses on traditional risk areas, overlooking cybersecurity risks, or that it lacks the required skills to perform cybersecurity audits. Enterprise risk management is enhanced by audits that identify technology users who either have a sense of invincibility towards cyber threats and exploits or believe that urgent job demands justify bypassing official cybersecurity standards (Stafford, Deitz and Li, 2018).

Information Technology

IT relationship quality was developed as the first sub-theme of information technology. Steinbart *et al.* (2013) and Wu *et al.* (2024) claimed that the quality of the relationship between internal audit and information security is positively influenced by information security professionals' perceptions of the value provided by the internal audit function. This suggests that auditors can enhance the implementation of audit findings related to information security by fostering a positive relationship with the information security department. Besides that, Steinbart *et al.* (2018) discovered that good relationship between the internal audit and information security function is improving the organization's collaborative detection capability both before and after they cause material harm.

IT governance process is the second sub-theme. The study from Wu *et al.* (2024) reveals that improved IAF-IT governance can enhance general controls, confirming the importance of IT governance audits conducted by IAFs. These audits evaluate the interplay of IT strategy, processes, risks, and control mechanisms. By understanding IT risks, IAFs can suggest suitable controls, ensuring effective risk management and alignment of organizational IT goals with overall business strategy, thus confirming the significance of IAF involvement in IT governance.

Technology audit is the third sub-theme. Technological advancements are crucial for establishing an effective digital auditing system, with data protection measures and employee skills significantly impacting cyber-attacks. Emphasis should be placed on preparing and building virtual auditing teams (Lois *et al.*, 2020). Internal audit departments are gradually using advanced technology like data analytics tools, recognising digital skills as a crucial asset (Betti and Sarens, 2020). The efficacy of consulting activities is positively impacted by the organization's level of digitalisation, as the IAF employs a greater number of data analytics technologies. Organisations that are experiencing digital transformation must address modifications in strategy, processes, and risks. In the context of an increasingly digitalised environment, the IAF could demonstrate its added value by assisting the organisation in anticipating risks and enhancing its business performance through the performance of consulting activities by internal auditors (Betti, Sarens and Poncin, 2021).

Management Action

Provide training was developed as the first sub-theme. It is crucial for auditors to possess the necessary IT training and experience to conduct an accurate assessment of controls (Curtis *et al.*, 2009). Wallace *et al.* (2011) shows that the management provide training to its internal audits employee can enhance their ability to identify and assess organisation control. The absence of training cause the inability internal audit to adapt to the new digitalised

environment (Lois *et al.*, 2020) relate to cyber security. However, Lois *et al.* (2021) mentioned It is clear that auditors who are trained in the prevention of cyber security risks may not be as effective in actual cybernetic attack scenario.

The second sub-theme is top management support, was developed as of the management action. Top management support is the supportive attitude of the management in terms of resources committed, participation in auditing plans, and serving as a role model in the workplace (Alazzabi *et al.*, 2023). The degree of dedication from senior management towards security is believed to significantly influence the overall efficiency of the organization's information security efforts (Hawkey, Muldner and Beznosov, 2008). Top management was supportive of information security in principle. Top management significantly influences the relationship between internal audit and information security staff. A "partnering" attitude between these executives leads to more collaborative relationships, whereas a less positive relationship between the two functions results in less effective collaboration (Steinbart *et al.*, 2012). The board of directors know the importance of cyber threat, give support to the IAF regarding the organization's governance procedures and policies is associated with cybersecurity audit (Islam *et al.*, 2018). Steinbart *et al.* (2018) stated that increased top management support for information security directly impacts organizations' efforts, reducing internal control weaknesses and employee non-compliance with IT policies, and thus improving overall security effectiveness. The top management are responsible for ensuring the company's top priorities, security, and resilience. Top management monitors privacy risks, including cybersecurity, financial, and organizational risks. They review information technology security design, implementation, and strategic decisions, and establish a security governance framework to ensure the company's security and resilience (Gunawan *et al.*, 2023).

Discussion

Internal auditors have the important role in evaluate and mitigate the level of IT and cybersecurity risks present in their organization by performing cyber security assessment. Figure 2 shows the propose framework to improve cyber security assessment through internal audit within organisations.

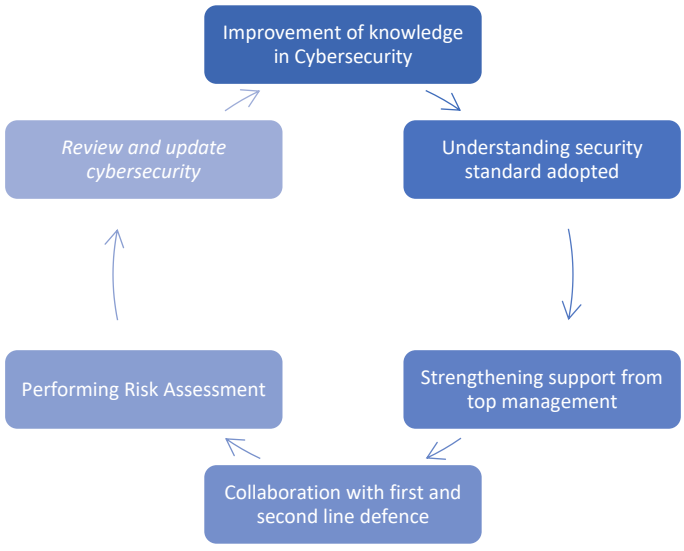

Figure 2. Proposed framework to improve cyber security assessment through internal audit
Source (s): Authors' creation

Improvement knowledge in Cybersecurity

Internal auditors who possess sufficient IT auditing experience, knowledge, skills, and training are able to more effectively comprehend the operation of information systems and the vulnerabilities of internal controls, thereby making a more significant contribution to the planning and execution of IT audits than those who lack this knowledge (Wu *et al.*, 2024). Wu *et al.* (2017) demonstrate that internal auditors can indirectly improve internal audit performance by enhancing IT audits if they possess a sufficient level of IT knowledge. Internal auditors need to participate in training seminars relate cyber security to improve their understanding in cybersecurity. Besides that, certification and training programs can serve as a form of capacity development for human resources in the cybersecurity sector, which is beneficial for the enhancement of cybersecurity (Gunawan *et al.*, 2023).

Understanding security standard adopted

The internal audit function should evaluate the efficacy and adequacy of the cyber security measures implemented by organizations in light of the existing frameworks they have implemented (PWC, 2023). The security standard that internal audit can evaluate against is established by the adopted frameworks, which in turn determines the cyber security postures of organizations (Jamison, Morris and Wilkinson, 2018). The top and commonly used cyber security frameworks adopted by organisations are discussed below for internal audit to use during their cyber security assessment. ISO (International Organization for Standardization, 27,000–31,000) (Duncan and Whittington, 2014), COBIT (Control Objectives for Information and related Technology) (Duncan and Whittington, 2014), SOX Act–COSO (Sarbanes Oxley) (Wallace, Lin and Cefaratti, 2011), NIST CSF (National Institute of Standards and Technology–Cybersecurity Framework)(Ibrahim *et al.*, 2018), IAABS (International Auditing and Assurance Standards Board) (Burgemeestre, Hulstijn and Tan, 2013), PCI-DSS (Payment Card Industry Data Security Standard) (Steinbart *et al.*, 2012) and CSAM (A Comprehensive Cybersecurity Audit Model). The understanding of security standard able to enhance the cyber security assessment performed by the internal audit (Steinbart *et al.*, 2018).

Strengthening Support from Top Management

The overall security of an organization is enhanced by the active participation of senior management in the resolution of security issues (Steinbart *et al.*, 2018).The internal audit will function efficiently if it received adequate recognition, acknowledgment, and appreciation by the top management (Alzeban and Gwilliam, 2014). Internal audit is essential for the organization's control environment and risk assessment, as it provides constructive services (Sinha and Arena, 2020). At present, numerous organizations are strengthen to fortify and assist their internal auditors by implementing a variety of strategies to ensure optimal performance. This includes providing sufficient budgetary allocations for training programs and facilitating access to advanced technological tools (Alqudah, 2023).

Collaboration with first and Second Lines of Defence

The internal audit function should collaborate with the first and second line of defence to reduce the significant cyber risks from materialising (PWC, 2023). The internal audit function plays an important role in coordinating with the first and second lines of defences to evaluate

the effectiveness and adequacy of controls to mitigate the cyber security risks (Delloite, 2017). The relationship between the internal audit and information security functions as second line of defence may also be positively impacted by the extent of senior management support as first defence for information security (Steinbart *et al.*, 2018). The association between the enhancement of IAFs' and IT relationship quality and IAF-IT governance process can boost IT control has been proved by Wu *et al.* (2024). IAFs can participate in cross-departmental meetings to discuss IT strategies, risk assessments, audit planning, compliance, and implemented controls. This proactive role enhances IT governance and internal control mechanisms, strengthening organizations' resilience against potential IT risks.

Performing Risk Assessment

Slapničar *et al.* (2022) mentions that vital role of internal audit function play in assisting the organisations in understanding and managing cyber security risks by evaluating the cyber security risk assessment. Management is provided with objective and independent assurance on governance, risk management, and controls by the internal audit function, which serves as the third line of defence. The internal audit function conducts an impartial evaluation of the effectiveness of the cyber risk assessment program and the cyber risk management processes (PWC, 2023). The third line defence included the assessment of the overall effectiveness of corrective measures taken by management in implementation of effective cyber risks management process to mitigate cyber risk and threats (Jamison, Morris and Wilkinson, 2018). The role of internal audit assists the organisations by providing an objective evaluation of the control and making recommendations in responding to cyber risks by evaluating the adopted organisation's cyber security programme (Steinbart *et al.*, 2018)

There are seven steps to explain the role of internal audit in cyber risk management is critical to ensuring effective oversight and providing independent assurance as follows:

1. Risk Assessment - The risk assessment process consists of three elements, namely (1) risk identification, by using checklists, consideration based on experience and documents, benchmarking, flow charts, brainstorming, system analysis, scenario analysis (2) risk analysis, and (3) risk evaluation (Gunawan *et al.*, 2023). Internal auditors should be competent to proactively identify emerging cybersecurity risk so internal audit should understand full impact of cyber threats on the organisations (Kahyaoglu and Caliyurt, 2018).
2. Audit Planning - One of the initial stages that internal audit must take in the development of a cybersecurity audit plan is to gain a comprehensive understanding of the cybersecurity framework that the organization employs. The selection of a framework is a management decision (Jamison, Morris and Wilkinson, 2018).
3. Control evaluation - Internal control testing checks the policies, procedures, practices, and organizational structures designed to identify the missing controls and evaluate physical control, administrative control and data control (Al-matari, Helal and Mazen, 2020).
4. Incident response review – Internal audit should maintains control during incident and doing investigation how to prevent in future incident happened (KPMG, 2019).
5. Compliance monitoring - The cybersecurity compliance process evaluates the security controls in organizational information systems on a regular basis to ascertain the efficacy of the controls in their application (Al-matari, Helal and Mazen, 2020).

6. Reporting and communication – Report security related internal control weakness and non-compliance incidents to top management (Steinbart *et al.*, 2018) and conveying risk and control information to relevant departments inside the organization; and organizing and sharing information between the board, external and internal auditors, and management (IIA, 2017).
7. Continuous improvement - A strong system of internal audits, designed to add value and improve procedures plays a key role in preventing next cyber-attacks (Drogalas, Arampatzis and Anagnostopoulou, 2016).

Review and update cybersecurity

Cybersecurity is a field that is constantly and quickly changing due to technology drive changes (KPMG, 2024). Internal auditors must stay updated on cybersecurity threats, technologies, and regulatory changes through professional development opportunities like training courses, conferences, and webinars. (IIA, 2021). Internal auditors should enhance their IT audit capabilities to offer proactive insights and value-added recommendations to management. They should stay updated on upcoming regulations, requirements, and industry trends, ensuring cyber security audit programs consider these changes (Kahyaoglu and Caliyurt, 2018).

Implications

This SRL able describes the factors that explain relationship between internal audit and cyber security (RQ1) and creating a framework for internal audit to improve cyber security assessment (RQ2). These findings are important for theoretical developments in field of auditing and cyber security, as they provide understanding of internal audit characteristics, internal audit role, information technology and management action that shapes an internal audit approach to cyber security assessment. Researcher and PR actioners can draw from these insights to develop more sophisticated models that capture the relationship between internal audit and cybersecurity in

The insight from RQ1 provide significant implications for internal audit seeking to enhance their work in cyber security assessment. By understanding the internal audit characteristics that impact to the quality of risk assessment, the organizations aware to provide training and support continuously to the internal audit function and IT function in order to improve IT knowledge, IT competencies and compliance of the security standards. The Companies need to invest significant in internal audit to acquire new resources and knowledge to assess cyber security dangers in order to prevent cyber-attack. From the internal audit role aspect, give insight to internal audit that the importance of their role as advisory, assurance and also risk management, so they can arrange the effective planning audit to fulfil objectives of those roles. From the aspect of information technology, in order to enhance the clarity of the auditor's role, it is necessary to update future audit standards to reflect the latest technology from the perspective of information technology.

In addressing RQ2, this research contributes to the development of comprehensive framework for internal auditor at enhancing cybersecurity assessment within organisations. These findings can serve as valuable input for audit committee and management of the organizations to revise the cyber security standards and audit guidelines. A refined standards and audit guidelines can accommodate the dynamical technology changes in business

process that prevent loss occurred from cyber attaches. Besides that, Chief Internal Audit can use these insights to create the effective audit plan and keep upgrade knowledge in cyber security in order to be able perform better quality audit of cyber security. The role of internal audit is not as compliance, but they have important role to reduce the risks from cyber threats by assessing cyber riks.

Limitation and Recommendations

Although Scopus, the most prominent database, has undertaken a comprehensive and ongoing review, it is still possible that significant articles were overlooked. The search was restricted to English-language publications published between 2011 and 2024, and papers in other languages were excluded. The keywords were selected in accordance with the study's scope. The SRL may have omitted certain critical items, despite the inclusion of cybersecurity and internal audit in the keyword selection.

The research that discuss internal audit and cybersecurity is still lacking. Future studies can pay more intention to how internal audit can anticipate provide independent perspectives into its company's ability to make compliant disclosures in this new era of cyber transparency because new rule of Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure released on July 26, 2023. Moreover, future research should focus on an analysis of the recommendations made by the internal audit function on cyber security and its impact on the organisations and evaluation on different organisations to determine the extent of implementation of internal audit recommendations relating to cyber security. Also, the studies can focus on the reliance of external audit on internal audit finding regarding weakness in cyber security in order to contribute theoretical from perspective of external audit. Besides that, future research can focus on the determinants of quality of advisory and assurance of internal audit in cyber security governance. Another promising area is examining the interactions of internal audit with audit committee and how these interactions affect the financial reporting quality. Another area that needs the attention of scholars is use of artificial intelligence, big data and block chain in internal auditing assessment on cyber security. Internal audit needs to understand use of fintech by examine how automated accounting software that can reduce errors and improve financial procedures.

Conclusion

The main purpose of this research is to examine the existing literature to get detailed understanding of the relationship between internal audit and cyber security. Through a systematic literature review, the author identified four main themes: internal audit characteristics, internal audit role, information and technology and management action. The authors proposed a comprehensive framework to improve cyber security assessment through internal audit based on these findings. The identified framework of cyber security assessment would help organizations worldwide proactively consider their strategy audit cyber security, recommendation and input from internal audit become basis for evaluate the cyber security policies. This research makes theoretical contribution in understanding the role of internal audit as one of the important aspects in explaining cyber security assurance. Cyber security is an important function that requires internal audit function to assist the organisations in evaluating the effectiveness and adequacy of controls to mitigate the impact of cyber security risks.

References

Al-matari, O. M. M., Helal, I. M. A., and Mazen, S. A. (2020) 'Integrated framework for cybersecurity auditing', *Information Security Journal: A Global Perspective*, 30(4), pp. 189–204. Available at: https://doi.org/10.1080/19393555.2020.1834649.

Alazzabi, W. Y. E., Mustafa, H., and Karage, A. I. (2023) 'Risk management , top management support , internal audit activities and fraud mitigation support', *Journal of Financial Crime*, 30(2), pp. 569–582. Available at: https://doi.org/10.1108/JFC-11-2019-0147.

Alqudah, H. (2023) 'The Mediating Role of Digital Competency between Top Management Support and the Electronic Internal Audit Tasks ' Effectiveness', *Intenational Journal of Academic Accounting, Finance & Management Research*, 7(12), pp. 71–80.

Alzeban, A., and Gwilliam, D. (2014) 'Factors affecting the internal audit effectiveness : A survey of the Saudi public sector', *Journal of International Accounting, Auditing and Taxation*, 23(2), pp. 74–86. Available at: https://doi.org/10.1016/j.intaccaudtax.2014.06.001.

Betti, N., and Sarens, G. (2020) 'Understanding the internal audit function in a digitalised business environment', *Journal of Accounting and Organizational Change*, 17(2), pp. 197–216. Available at: https://doi.org/10.1108/JAOC-11-2019-0114.

Betti, N., Sarens, G., and Poncin, I. (2021) 'Effects of digitalisation of organisations on internal audit activities and practices', *Managerial Auditing Journal*, 36(6), pp. 872–888. Available at: https://doi.org/10.1108/MAJ-08-2020-2792.

Braun, V., and Clarke, V. (2019) 'Reflecting on reflexive thematic analysis', *Qualitative Research in Sport, Exercise and Health*, 11(4), pp. 589–597. Available at: https://doi.org/10.1080/2159676X.2019.1628806.

Burgemeestre, B., Hulstijn, J., and Tan, Y. H. (2013) 'Value-based argumentation for designing and auditing security measures', *Ethics and Information Technology*, 15(3), pp. 153–171. Available at: https://doi.org/10.1007/s10676-013-9325-2.

Curtis, M. B. (2009) 'Auditors' training and proficiency in information systems: A research synthesis', *Journal of Information Systems*, 23(1), pp. 79–96. Available at: https://doi.org/10.2308/jis.2009.23.1.79.

Delloite. (2017) 'Cybersecurity and the role of internal audit - An urgent call to action', p. 10. Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-cyber-ia-urgent-call-to-action.pdf.

Drogalas, G., Arampatzis, K., and Anagnostopoulou, E. (2016) 'The relationship between corporate governance, internal audit and audit committee : Empirical evidence from Greece', *Corporation Ownership & Control*, 14(1), pp. 569–577.

Duncan, B., and Whittington, M. (2014) 'Compliance with standards, assurance and audit: Does this equal security?', *ACM International Conference Proceeding Series*, (April), pp. 77–84. Available at: https://doi.org/10.1145/2659651.2659711.

Elmaasrawy, H. E., and Tawfik, O. I. (2024) 'Impact of the assertive and advisory role of internal auditing on proactive measures to enhance cybersecurity: evidence from GCC', *Journal of Science and Technology Policy Management* [Preprint]. Available at: https://doi.org/10.1108/JSTPM-01-2023-0004.

Gunawan, B. (2023) 'Cybersecurity effectiveness: The role of internal auditor certification, risk assessment and senior management', *International Journal of Data and Network Science*, 7(4), pp. 1805–1814. Available at: https://doi.org/10.5267/j.ijdns.2023.7.011.

Haddaway, N. R. (2018) 'ROSES Reporting standards for Systematic Evidence Syntheses: Pro

forma, flow-diagram and descriptive summary of the plan and conduct of environmental systematic reviews and systematic maps', *Environmental Evidence*, 7(1), pp. 4–11. Available at: https://doi.org/10.1186/s13750-018-0121-7.

Hawkey, K., Muldner, K. and Beznosov, K. (2008) 'Searching for the right fit: Development of applicant person-organization', *IEEE Internet Comput*, pp. 22–30.

Héroux, S., and Fortin, A. (2013) 'The internal audit function in information technology governance: A holistic perspective', *Journal of Information Systems*, 27(1), pp. 189–217. Available at: https://doi.org/10.2308/isys-50331.

Hong, Q. N. (2018) 'The Mixed Methods Appraisal Tool (MMAT) version 2018 for information professionals and researchers', *Education for Information*, 34(4), pp. 285–291. Available at: https://doi.org/10.3233/EFI-180221.

Ibrahim, A. (2018) 'A security review of local government using NIST CSF: a case study', *Journal of Supercomputing*, 74(10), pp. 5171–5186. Available at: https://doi.org/10.1007/s11227-018-2479-2.

IIA (2017) 'International Standards For The Professional Practice Of Internal Auditing (Standards)', (October 2016), pp. 1–25.

IIA (2020) 'THE IIA ' s Three Line s Model An update of the Three Lines of Defense', *Global Headquarters The Institute of Internal Auditors*, p. 13.

IIA (2021) *Persevering in a pandemic internal auditors are adapting to change and meeting extraordinary challenges head-on*.

Islam, M. S., Farah, N., and Stafford, T. F. (2018) 'Factors associated with security/cybersecurity audit by internal audit function: An international study', *Managerial Auditing Journal*, 33(4), pp. 377–409. Available at: https://doi.org/10.1108/MAJ-07-2017-1595.

Jamison, J., Morris, L., and Wilkinson, C. (2018) 'The future of cybersecurity in internal audit research report by the internal audit foundation and crowe horwath'. Available at: https://graces.community/wp-content/uploads/2022/01/1640227244602.pdf.

Kahyaoglu, S., and Caliyurt, K. (2018) 'Cyber security assurance process from the internal audit perspective', *Managerial Auditing Journal*, 33(4), pp. 360–376. Available at: https://doi.org/10.1108/MAJ-02-2018-1804.

Kannelønning, K., and Katsikas, S. K. (2023) 'A systematic literature review of how cybersecurity-related behavior has been assessed', *Information and Computer Security*, 31(4), pp. 463–477. Available at: https://doi.org/10.1108/ICS-08-2022-0139.

Kiger, M. E., Meyer, H. S., and Varpio, L. (2021) '"It is you, me on the team together, and my child": Attending, resident, and patient family perspectives on patient ownership', *Perspectives on Medical Education*, 10(2), pp. 101–109. Available at: https://doi.org/10.1007/s40037-020-00635-8.

Kitchenham, B. (2009) 'Systematic literature reviews in software engineering - A systematic literature review', *Information and Software Technology*, 51(1), pp. 7–15. Available at: https://doi.org/10.1016/j.infsof.2008.09.009.

KPMG. (2019) 'The role of internal audit in cyber security readiness'.

KPMG. (2024) 'Technology risk and its impact on internal audit'.

Kraus, S., Breier, M., and Dasí-Rodríguez, S. (2020) 'The art of crafting a systematic literature review in entrepreneurship research', *International Entrepreneurship and Management Journal*, 16, pp. 1023–1042.

Lockwood, C., Munn, Z., and Porritt, K. (2015) 'Qualitative research synthesis: Methodological guidance for systematic reviewers utilizing meta-aggregation', *International Journal of*

Evidence-Based Healthcare, 13(3), pp. 179–187. Available at: https://doi.org/10.1097/XEB.0000000000000062.

Lois, P. (2020) 'Internal audits in the digital era: opportunities risks and challenges', *EuroMed Journal of Business*, 15(2), pp. 205–217. Available at: https://doi.org/10.1108/EMJB-07-2019-0097.

Lois, P. (2021) 'Internal auditing and cyber security: Audit role and procedural contribution', *International Journal of Managerial and Financial Accounting*, 13(1), pp. 25–47. Available at: https://doi.org/10.1504/IJMFA.2021.116207.

Okoli, C. (2015) 'A guide to conducting a standalone systematic literature review', *Communications of the Association for Information Systems*, 37(1), pp. 879–910. Available at: https://doi.org/10.17705/1cais.03743.

Patterson, C. M., Nurse, J. R. C., and Franqueira, V. N. L. (2023) 'Learning from cyber security incidents: A systematic review and future research agenda', *Computers and Security*, 132. Available at: https://doi.org/10.1016/j.cose.2023.103309.

Podsakoff, P. M. (2005) 'The influence of management journals in the 1980s and 1990s', *Strategic Management Journal*, 26(5), pp. 473–488. Available at: https://doi.org/10.1002/smj.454.

PWC. (2023) 'Cybersecurity disclosures and the role of internal audit', (August), pp. 1–5.

Rahim, N. H. A. (2015) 'A systematic review of approaches to assessing cybersecurity awareness', *Kybernetes*, 44(4), pp. 606–622. Available at: https://doi.org/10.1108/K-12-2014-0283.

Rodgers, W., Alhendi, E., and Xie, F. (2019) 'The impact of foreignness on the compliance with cybersecurity controls', *Journal of World Business*, 54(6), pp. 1–11. Available at: https://doi.org/10.1016/j.jwb.2019.101012.

Rohan, R. (2023) 'A systematic literature review of cybersecurity scales assessing information security awareness', *Heliyon*, 9(3), pp. 1–26. Available at: https://doi.org/10.1016/j.heliyon.2023.e14234.

Shaffril, H. A. M., Samah, A. A., and Samsuddin, S. F. (2021) 'Guidelines for developing a systematic literature review for studies related to climate change adaptation', *Environmental Science and Pollution Research*, 28(18), pp. 22265–22277. Available at: https://doi.org/10.1007/s11356-021-13178-0.

Sinha, V. K., and Arena, M. (2020) 'Manifold conceptions of the internal auditing of risk culture in the financial sector', *Journal of Business Ethics*, 162(1), pp. 81–102. Available at: https://doi.org/10.1007/s10551-018-3969-0.

Slapničar, S. (2022) 'Effectiveness of cybersecurity audit', *International Journal of Accounting Information Systems*, 44, pp. 1–21. Available at: https://doi.org/10.1016/j.accinf.2021.100548.

Stafford, T., Deitz, G., and Li, Y. (2018) 'The role of internal audit and user training in information security policy compliance', *Managerial Auditing Journal*, 33(4), pp. 410–424. Available at: https://doi.org/10.1108/MAJ-07-2017-1596.

Steinbart, P. J. (2012) 'The relationship between internal audit and information security: An exploratory investigation', *International Journal of Accounting Information Systems*, 13(3), pp. 228–243. Available at: https://doi.org/10.1016/j.accinf.2012.06.007.

Steinbart, P. J. (2013) 'Information security professionals' perceptions about the relationship between the information security and internal audit functions', *Journal of Information Systems*, 27(2), pp. 65–86.

Steinbart, P. J. (2016) 'SECURQUAL: An instrument for evaluating the effectiveness of

enterprise information security programs', *Journal of Information Systems*, 30(1), pp. 71–92. Available at: https://doi.org/10.2308/isys-51257.

Steinbart, P. J. (2018) 'The influence of a good relationship between the internal audit and information security functions on information security outcomes', *Accounting, Organizations and Society*, 71, pp. 15–29. Available at: https://doi.org/10.1016/j.aos.2018.04.005.

Taylor, P. J. 2020) 'A systematic literature review of blockchain cyber security', *Digital Communications and Networks*, 6(2), pp. 147–156. Available at: https://doi.org/10.1016/j.dcan.2019.01.005.

Tober, M. (2011) 'PubMed, ScienceDirect, Scopus or Google Scholar - Which is the best search engine for an effective literature research in laser medicine?', *Medical Laser Application*, 26(3), pp. 139–144. Available at: https://doi.org/10.1016/j.mla.2011.05.006.

Wallace, L., Lin, H., and Cefaratti, M. A. (2011) 'Information security and sarbanes-oxley compliance: An exploratory study', *Journal of Information Systems*, 25(1), pp. 185–211. Available at: https://doi.org/10.2308/jis.2011.25.1.185.

Wu, T. H. (2017) 'The effect of competencies, team problem-solving ability, and computer audit activity on internal audit performance', *Information Systems Frontiers*, 19(5), pp. 1133–1148. Available at: https://doi.org/10.1007/s10796-015-9620-z.

Wu, T. H. (2024) 'IT governance and IT controls: Analysis from an internal auditing perspective', *International Journal of Accounting Information Systems*, 52, pp. 1–16. Available at: https://doi.org/10.1016/j.accinf.2023.100663.