Jurnal TRANSFORMATIKA
Vol.23, No.2, Januari 2026, pp. 135 - 154
P-ISSN: 1693-3656, E-ISSN: 2460-6731
https://journals.usm.ac.id/index.php/transformatika/

Cyber Security Audit in Information Technology Governance: A Literature Review and Future Research Agenda

Nazri Sidqi Fachriaz[1], Saifudin Saifudin[2*]
[1]Dian Nuswantoro University/Informatics
Jalan Imam Bonjol 207 Semarang, +62 (024) 3517261, e-mail: 111202516125@mhs.dinus.ac.id
[2]Universitas Semarang (USM)/Accounting
Jalan Soekarno Hatta Semarang, +62 (024) 6702757, e-mail: saifudin@usm.ac.id

ARTICLE INFO

History of the article :
Received 23 Agustus 2025
Received in revised form 20 Desember 2026
Accepted 9 Januari 2026
Available online 30 Januari 2026

Keywords:

cyber security audit; information technology governance (ITG); systematic literature review; future research agenda.

*** Correspondence:**

Telepon:
+62 (024) 6702757

E-mail:
saifudin@usm.ac.id

ABSTRACT

This study aims to examine cyber security audits in information technology governance (ITG) more deeply using a literature review approach. The method used in this research is a systematic literature review by applying PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analysis) method approach with 25 years of observation from 1999 to 2024. 980 articles were obtained, nevertheless, only 36 articles were eligible. The research results show that cyber security audit is compatible and closely related to information technology governance (ITG), mainly the domain regarding the need for the board of directors to understand and to master cyber security audit skills to overcome violations and data leaks in IT governance. Cyber security audit and information technology governance (ITG) are two key components to maintain information security as well as to manage information technology effectively. Integration between the two in a conceptual framework helps organizations identify, manage and mitigate cyber risks and maintain alignment with business objectives.

1. INTRODUCTION

Current digital era has brought unprecedented levels of connectivity, convenience and innovation, but also new risks, mainly in the form of cyber threats. The ever-evolving nature of cyber threats presents significant challenges for all entities [1]. It is essential for all entities to combine strong cyber security audit practices with information technology governance (ITG) principles to maintain information security and to run business operations smoothly as well [2].

Cyber security audit is a process of monitoring systems, networks, and information security practices to identify potential threats and to evaluate existing levels of protection [3], [4], while ITG is a structure which directs decision making and management of IT resources to achieve organizational goals [5]. Both domains have a crucial role for managing risk, ensuring compliance, and improving operational efficiency [4], [6], [7]. Therefore, developing a conceptual framework which combines the two is an essential step for any entities in today's dynamic modern era. The following figure 1 is an overview of the latest mapping of the relationship between cyber security audit and ITG:

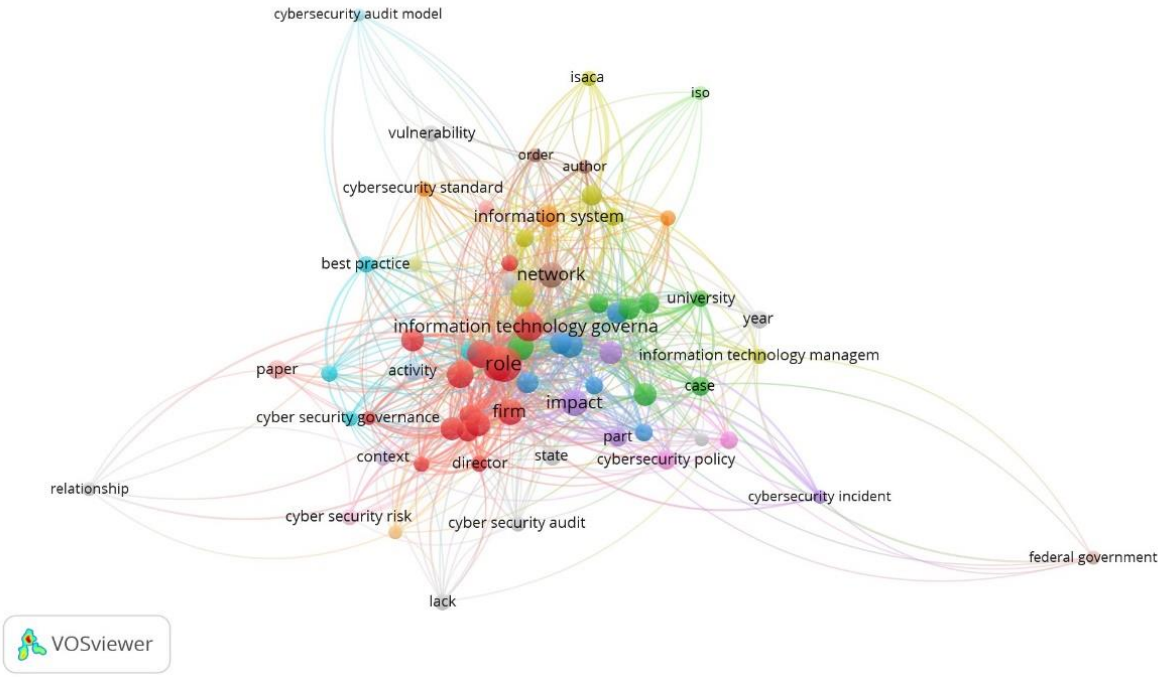

Figure 1. Mapping the relationship between cyber security audit and ITG by theme
Source: VOS viewer, 2025

As seen in figure 1 above, it can be stated that ITG is central to the studies which are most widely used as research material. Moreover, when closely observed, cyber security is the variable which has the most connectivity associated with ITG. Figure 2 shows recent themes that can be associated with ITG.

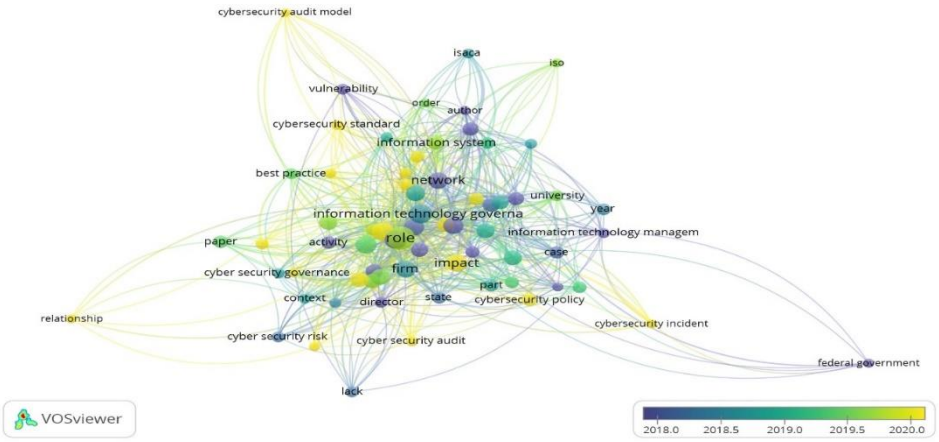

Figure 2. Mapping the relationship between cyber security audit and ITG by years
Source: VOS viewer, 2025

Based on Figure 2, studies from the most recent years, i.e. 2020 and above, which is symbolized by a yellow point image, show that the theme of cyber security audit is the most central theme used as material for studies and research related to ITG. Following to these facts, this research is aimed to examine cyber security audits in ITG more deeply using a literature review approach.

Cyber security Audit

Cyber security audit is a systematic and structured process for evaluating the level of security of an organization against cyber threats [3], [8]–[11]. This cyber security audit involves data collection, risk analysis, and examination of policies and security practices [4], [6], [7]. The results of the audit are used to identify weaknesses and to design necessary improvements [12]. In addition, the steps taken include data collection, i.e. by collecting information about systems, networks and security practices that exist within the organization. Furthermore, a risk analysis is conducted, i.e. by analysing potential threats and their impact on the organization. The next step is compliance evaluation, namely checking the organization's compliance with security standards and applicable regulations by identifying weaknesses, which then need to be corrected. The final stage is reconstruction and improvement, i.e. implementing changes and improvements to enhance the security.

Information Technology Governance (ITG)

ITG is a framework that helps organizations manage IT resources effectively [5], [13]–[15]. The goal is to ensure that information technology supports business objectives, manages risks well, and complies with applicable regulations [16]. ITG involves components, including: first, leadership and strategy on IT by developing an IT vision and strategy that supports organizational goals; second, measuring performance by monitoring and measuring IT performance to ensure efficiency and effectiveness; third, risk management is carried out by identifying, evaluating and managing risks related to IT; and the fourth one, internal control by implementing internal control to protect IT assets and ensure compliance.

Integration of Cyber security Audit with ITG

A conceptual framework that combines cyber security audit and ITG to ensure that information security practices are aligned with organizational goals. Several ways of this integration can be elaborated as seen in Figure 3 below:

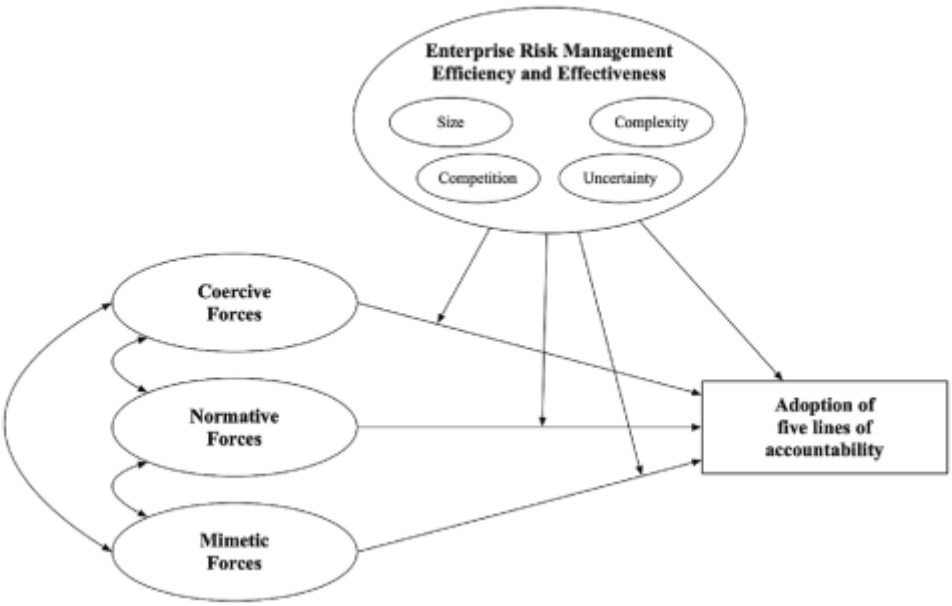

Figure 3. The conceptual framework of the adoption of the five lines of accountability
Source: [17]

RESEARCH METHODS

In this research, the approach used is a systematic literature review (SLR). SLR is a method of synthesizing scientific evidence to answer a specific research question in a transparent and reproducible way by incorporating all the evidence which has been published on the topic and assessing the quality of the evidence[18]. [18] also added that SLR has become the main methodology used in various scientific disciplines. These also include auditing [19]. The following are the stages of research using the SLR approach based on several references [20]–[22]. The steps in the searching stage are divided into several processes, i.e. identification, screening, eligibility and inclusion. This step is in accordance with the guidelines in PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analysis). PRISMA is a series of evidence-based minimums which aims to help report various systematic reviews and meta-analyses that assess benefits [22], [23].

Searching stage was conducted using Publish or perish (PoP) tools. PoP is a phrase that describes the pressure placed on academics to publish in scientific journals quickly and continuously as a condition for getting a job (looking for work), promotion, and even maintaining one's job [24].

The steps in SLR-based research are elaborated in Figure 4 as follows:

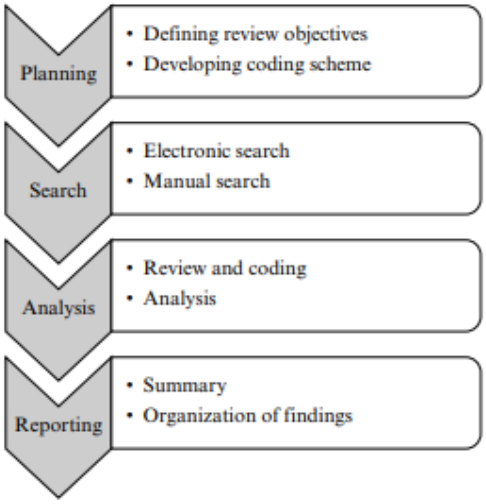

Figure 4. Steps in the systematic literature review

Source: [25]

In accordance with Figure 4 above, the first stage is planning or preparation. Preparation stage covers preparing the supporting tools used to process the articles to be selected. The tools prepared for searching actions are PoP and VOSviewer which have proven to be very relevant to use [26]. At this planning stage, there are research questions (RQ) proposed, i.e. how is cyber security audit used in ITG? (RQ1) and what cyber security audit domains are used in ITG? (RQ2). The second stage is literature searching, i.e. the process of obtaining relevant research articles to obtain answers to research questions [19]. The following databases were selected for the literature searching: 1) Science Direct, 2) Scopus.com, 3) Google Scholar. Selected articles range from publication from 1999 to 2024. The literature search strategy used the keywords "CYBER SECURITY AUDIT" and "INFORMATION TECHNOLOGY GOVERNANCE (ITG)". The third stage is conducting analysis. In the analysis stage, the papers resulted from literature searching were selected by employing PoP application. The literatures obtained were then selected based on inclusion and exclusion criteria according to the needs used in this research. These criteria are as follow.

Inclusion criteria:

a) The language used is English
b) The articles are published in international journals between 1999 and 2024
c) The articles discuss about cyber security audit which is related and relevant to information technology governance
d) The articles are available in full text form

Exclusion criteria:

a) The articles are not available in full text form
b) The articles do not explain about cyber security audit which is related and relevant to information technology governance
c) The articles lack relevant research methods
d) The language used is not English

The fourth stage is reporting. Reporting stage includes providing a quality assessment of the scientific articles that have been selected by establishing quality criteria. The Quality Assessment (QA) criteria in this research are as follow:

- QA1: Does the paper contain the relationship between cyber security audit and ITG?

- QA2: Does the paper state the cyber security audit domain used in ITG?

RESULTS AND DISCUSSIONS

Based on the explanation of the stages in the research methodology previously elaborated, the SLR stages were carried out starting with planning and searching. Figure 5 shows an overview of study searching results using PoP:

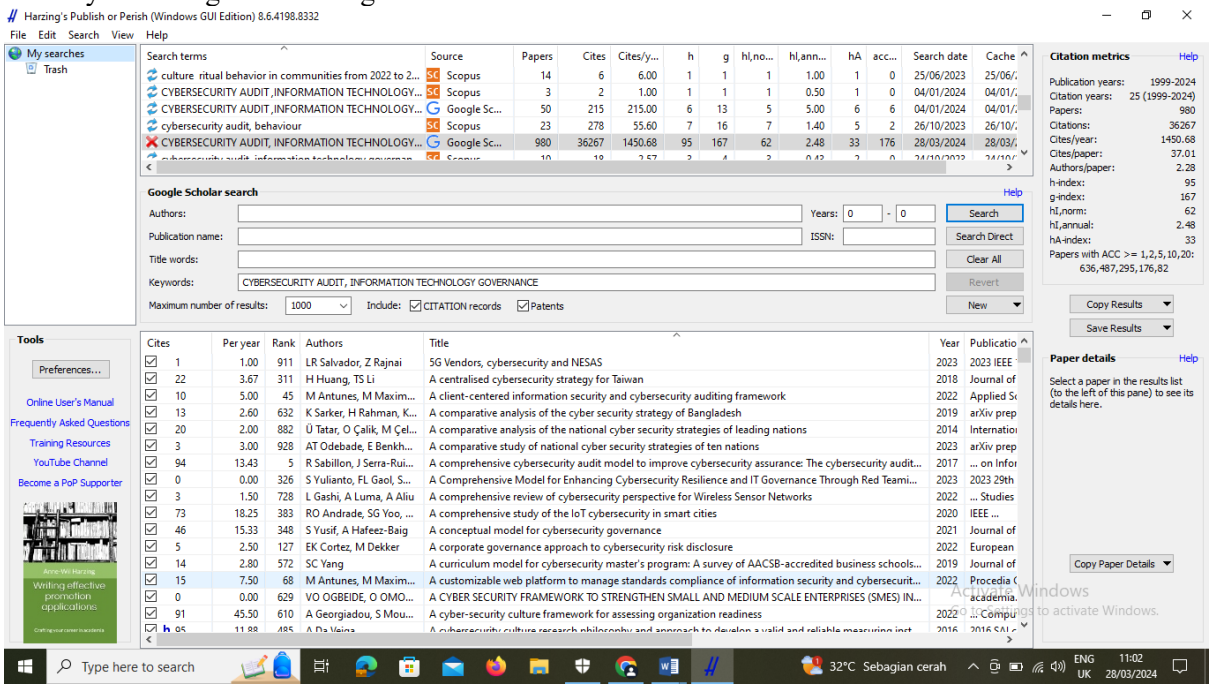

Figure 5. Results of the Search for the Relationship between Cyber security Audit and ITG in 1999-2024)

Source: Publish or Perish, 2025

According to the results of investigation on the relevant articles using publish or perish (PoP), 980 articles were obtained from 1999 to 2024 (a time span of 25 years). Searches using PoP are based on the keyword index used, i.e. “CYBER SECURITY AUDIT” and “INFORMATION TECHNOLOGY GOVERNANCE (ITG)”. From the 980 articles obtained, the SLR stage was then continued using the PRISMA method as described in this following Figure 6:

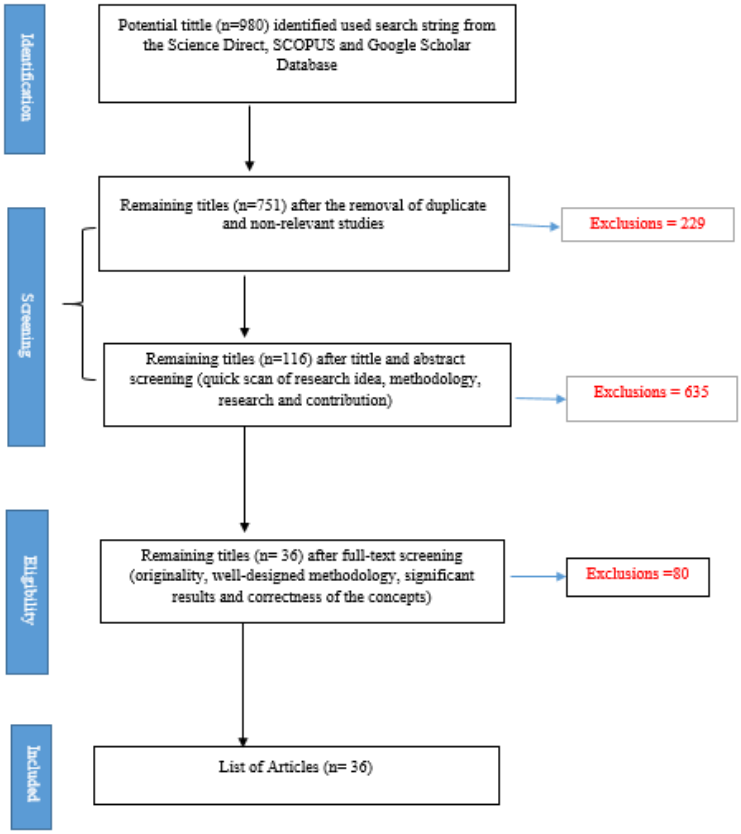

Figure 6. PRISMA Diagram
Source: personalized processed data, 2025

It can be concluded based on Figure 6 above that the identification results of 980 articles were successfully collected. Then, selection was carried out by sorting the data, i.e. checking the titles to avoid duplicate titles and articles whose studies were not relevant. This stage resulted in 751 relevant articles obtained. Furthermore, these 751 articles were analysed in more depth to obtain relevant data. The expected data criteria were that the article must have research ideas relevant to this research topic, i.e. cyber security audit and ITG, and should have research methodology contributing to the theme. The selection stage resulted in the remaining titles, i.e.116 relevant articles. In the eligibility stage, only 36 articles were obtained. It is called eligible when the article has full text after screening, is original, has a good design in its methodology, significant research results, and has an appropriate and proper research concept. The 36 articles that were successfully obtained for themes corresponding to cyber security audit in ITG came from journals as seen in table 1 below:

Tabel 1. Breakdown of Reviewed Studies

Accounting, Organizations and Society	1
AMCIS 2017	1
Applied Sciences	1
Auditing: A Journal of Practise & Theory	1
Centeris 2021	1
Computer and Security	1
Continuity & Resilience Review	1
Current Issues in Auditing	1
Digital Policy, Regulation and Governance	2
Information and Computer Security	4
International Journal of Accounting Information Systems	4
International Journal of Critical Infrastructures	1
International Journal of Disclosure and Governance	1
Journal of Cybersecurity and Privacy	1
Journal of Information Systems	4
Journal of Management and Governance	2
Managerial Auditing Journal	4
Procedia Computer Science	1
Review of Accounting Studies	1
Sensors	2
SSRN Electronic Journal	1
Total	**36**

Source: personalized processed data, 2025

As seen in Table 1, it can be seen that the most studies on cyber security auditing in ITG were found in 4 articles concerning Information and Computer Security, International Journal of Accounting Information Systems, Journal of Information Systems and Managerial Auditing Journal. Furthermore, 2 articles are in the journals Digital Policy, Regulation and Governance, Journal of Management and Governance and Sensors. Apart from these journals, each submitted 1 article.

Based on the years studied, it turns out that the theme of cyber security audit in ITG has merged since 1999 and has only started to be researched in 2007. Thus, this theme has only been running for 17 years as shown in Figure 7 as follows:

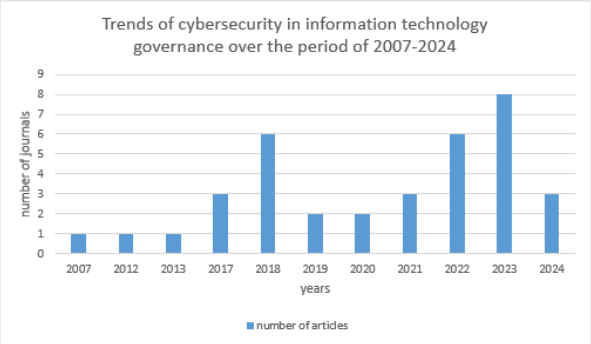

Figure 7. Trends of Cyber security in ITG Over Period of 2007-2024
Source: personalized processed data, 2025

As described in Figure, cyber security audit theme in ITG was most frequently found in 2023, i.e. 8 articles, followed by 2022 and 2018 respectively with 6 articles each. Furthermore, in 2017, 2021 and 2024 there are 3 articles each. Meanwhile, specifically for 2024, the data obtained is only available until April 2024 (by the time this study was conducted).

The following Figure 8 describes the research methodology carried out on the theme of cyber security audit in ITG:

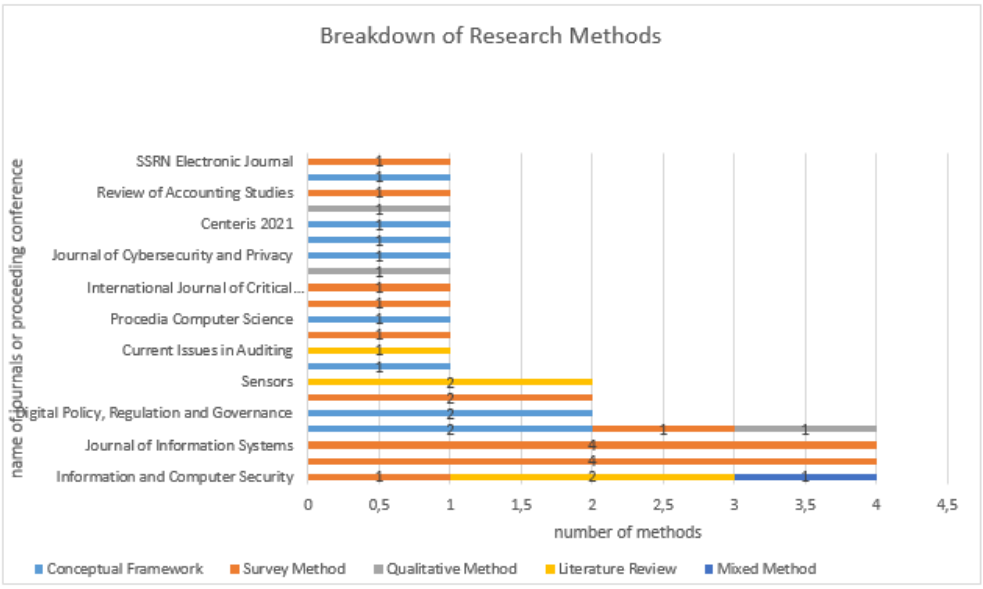

Figure 8. Breakdown of Research Methods
Source: personalized processed data, 2025

Figure 8 above describes that the cyber security audit theme in ITG mostly uses research methods with the survey method, i.e. 17 articles with 10 articles using the conceptual framework method. Furthermore, there were 5 articles using the literature review method and 3 articles using the qualitative method and only 1 article using a qualitative and quantitative mix-method.

The SLR study with the theme of cyber security in ITG resulted in 36 selected articles, which summarize the results and recommendations for future studies as discussed in the following Table 2:

Table 2. Summary of Research Results and Recommendations for Future Research

No.	Years	Author	Name of Journals	Research Results	Recommendations for Future Research
1	2007	[27]	International Journal of Accounting Information Systems	that there is a causal relationship between management and IT professionals are concerned with design, implementation, and assessment of IT governance strategies	Future research needs to check interviews at various levels of industry scale about IT governance, in addition it also needs to include external partners in IT governance, then also examine the attitudes of several business units towards IT governance in large and complex organisations. next also align IT governance with IT value drivers, and finally include conducting action research in the COBIT framework.
2	2012	[28]	International Journal of Accounting Information Systems	The research developed an exploratory model of factors that influence the nature of the relationship between between the internal audit function and information security, illustrating the potential benefits that organisations can derive from the relationship. benefits that organisations can derive from the relationship	Future research could reconfirm, as the nature of the relationship between internal audit and information security and information system security functions differs across the four institutions studied.
3	2013	[29]	Journal of Information Systems	that there is a positive relationship between information security and the internal audit function within organisations.	Future research could examine the relationship between information security and the internal audit function within organisations, by developing developing a more reliable measure of information security

					professionals' perceptions of the role of internal audit, and then adapting the instrument to measure internal auditors' perceptions of the role of internal audit.
4	2017	[30]	Digital Policy, Regulation and Governance	that a strong market and network governance structure that is more limited to the role of hierarchical structures can use purely hierarchical methods governance structure.	In the future, there needs to be an alignment of the private and government sectors in the implementation of cyber security, both in ex ante (before the incident) and ex post (after the incident) practices.
5	2017	[31]	AMCIS 2017	the need for a board of directors with IT governance security expertise in a business entity	there needs to be a board of directors with IT governance security expertise in a business entity, if there is none, then there needs to be an internal auditor who has this expertise.
6	2017	[32]	Digital Policy, Regulation and Governance	the results show that the private sector internalises some externalities, mostly on a voluntary basis and through network governance mechanisms. this is the first step in the development of cyber security.	Future research is needed to identify how these mechanisms can be expanded or augmented to further improve cyber security governance.
7	2018	[33]	Review of Accounting Studies	The findings of this research, found that undisclosed cyberattacks were associated with an approximate 3.6% drop in equity value in the month that the attack was discovered, and disclosed attacks had a much lower drop of 0.7%.	Future research is expected to add other variables to find out what factors cause the impact of cyber security on reducing equity.
8	2018	[34]	Managerial Auditing Journal	The result of this article is that there are four main cyber-focused standards and frameworks in the current literature, namely, Control Objectives for Information and Related Technology, International Organization for	Cyber risk is not something that can be avoided, but rather must be managed. Therefore, future research could consider internal audits as they are an integral part of the

				Standardization, The American Institute of Certified Public Accountants, and National Institute of Standards and Technology.	cyber security assurance process.
9	2018	[35]	Managerial Auditing Journal	the results showed that the level of cyber security audit is significantly and positively related to the Internal Audit Function's (IAF) competence in governance, risk, and control.	Future research could focus on the reasons for low audit committee involvement in cyber security audits.
10	2018	[36]	Managerial Auditing Journal	With a cyber security audit, companies benefit from risk management, especially from cyber threats and exploitation.	Future research can further develop this study. This study is the first study in characterising the notion of Cyber security Loafing.
11	2018	[37]	Accounting, Organizations and Society	that the quality of the relationship between the internal audit and information cyber security functions affects the an objective measure of the overall effectiveness of an organisation's information security efforts	an important topic for future research is to investigate the the effect of these internal audit quality measures, not only on the the relationship between the internal audit function and the information security function, but also on information security outcomes. rities, but also on information security outcomes.
12	2018	[38]	Information and Computer Security	The outcome of this article is to clearly define the relationship between cyber security and information security, especially from a governance perspective.	The limitation of this article is that it is based on ISO alone. so future research, can develop more outside ISO
13	2019	[39]	Managerial Auditing Journal	Cyber testing techniques provide insight into the effectiveness of implementing actual cyber security controls	With the presented cyber testing techniques complementing traditional process-oriented assurance techniques, future research can test cyber with other techniques.
14	2019	[40]	Journal of Information Systems	The research found that breaches are associated with increased costs, but	Future researchers can test with other methods or other

				the impact is driven by external breaches.	variables about whether auditors have the risk of price gouging into their fees and whether the company's internal governance can mitigate the potential increase in audit fees.
15	2020	[41]	International Journal of Critical Infrastructures	The results found that there is a significant and direct relationship between both ITG and the level of corporate cyber security	Future research needs to examine the factors that influence the need for a board of directors who master cyber security, have information technology knowledge and experience.
16	2020	[42]	Auditing: A Journal of Practise & Theory	This research found that only cyber incidents were associated with an increase in audit fees and the relationship was was driven by more severe incidents.	Future research is expected to use variables other than audit fees in relation to cyber incidents.
17	2021	[9]	CENTERIS	that information about frameworks in information security and cyber security that are based on such as ISO-27001:2013, the NIST Cyber security Framework and ISO-27009 is feasible and appropriate.	For future research, it is expected to improve the implementation of the framework that has been made, which refers to the ISO 27001: 2013-based audit project.
18	2021	[43]	Current Issues in Auditing	This research literature review provides evidence that board IT committees, management teams with IT expertise, and audit committees can play an active role in mitigating security breaches.	Further research is needed to understand how companies can better address and prevent the different types of cyber security breaches that affect organisations.
19	2021	[44]	SSRN Electronic Journal	Researchers found that normative power (cyber security certification of internal auditors) and human agency factors significantly explain the effectiveness of Cyber security Audits.	To establish the robustness of the findings, future research could measure isomorphic strength and human agency factors with alternative indicators or use different methodological approaches.
20	2022	[8]	Applied Sciences	The results of this study propose a generalised, client-centred cyber	For future research, it is expected to examine audits to

				security audit information system integrated with the web.	evaluate and mitigate information security risks with other method approaches.
21	2022	[45]	Journal of Management and Governance	The main findings of this study suggest that the presence of a committee responsible for cyber security on the board of directors is key to improving cyber security disclosures.	The results of this study, which show the relationship between various board characteristics and the overall level of cyber security disclosure as well as its individual aspects, can be further developed by future researchers with other variables.
22	2022	[46]	Information and Computer Security	The finding of this article is that each cyber security capability can be further operationalised with a set of cyber security controls derived from various frameworks, standards, and guidelines, such as COBITV R, CISV R, ISA/IEC 62443, ISO/IEC 27002, and NIST publication 800-53.	For future research, it is recommended that separate but integrated enterprise IT and ICS cyber security teams be established in one security operations centre.
23	2022	[47]	Procedia Computer Science	The outcome of this paper is to provide insights for strategic and tactical business decision support suitable for mitigating possible cyber security breaches and threats with a System Dynamics Modelling (SDM) approach.	The results of the framework in this study can be further developed by future researchers to open up insights for strategic and tactical business decision support suitable for mitigating possible cyber security breaches and threats.
24	2022	[11]	International Journal of Accounting Information Systems	The research found that cyber security Audit Index scores varied widely, with an average of 58 on a scale of 0 to 100. On the other hand, the planning and execution phases were strongly and positively correlated, but less associated with reporting on the effectiveness of cyber risk management to the Board of Directors.	In the future, it is necessary to improve in measuring the effectiveness of cyber security audits and their effect on cyber risk management.
25	2022	[48]	Computer and Security	This research proposes an architecture-based security conceptual	future research can develop an architecture-based security conceptual

				framework that has three components namely system representation model type, security representation model type, and security process model type.	framework that has three components namely system representation model type, security representation model type, and security process model type.
26	2023	[49]	Information and Computer Security	The result of this research is that not all financial analysts consider cyber security information in their investment analysis process and not all financial analysts find cyber security disclosures in corporate financial statements useful.	Future research can help define and develop measures for reliable and comparable quantitative and qualitative cyber security data
27	2023	[50]	Journal of Cyber security and Privacy	The framework developed in this research, incorporates various components that are not considered in existing frameworks, such as research and development, public-private collaboration framework, regional and international cooperation framework, incident management, business continuity, disaster recovery framework, and compliance with laws and regulations.	As a next step, the implementation, evaluation and validation of the proposed framework will be conducted in the selected organisations to see its effectiveness.
28	2023	[51]	Sensors	The result of this research is that a comprehensive framework is proposed for implementing cyber threat intelligence (CTI) in organisations.	Future research is expected to develop a comprehensive framework proposed for implementing cyber threat intelligence (CTI) in organisations that is tailored to the needs and resources available.
29	2023	[52]	Information and Computer Security	The findings of this study indicate that the Cyber Trust Programme (CTP) has a significant impact on the cyber security assurance of government entities participating in the CTP.	Future research is expected to evaluate how the cyber trust programme (CTP) improves managers' decision-making skills and competencies, as well as how resources are allocated and how the CTP is matched to organisational needs.

30	2023	[17]	International Journal of Accounting Information Systems	The researcher found that all the organisations studied adopted the 5 LoAs clearly to improve the effectiveness of cyber security governance.	Future research can develop 5 LoAs to improve the effectiveness of cyber security governance.
31	2023	[53]	Journal of Management and Governance	This research finds evidence that effective boards has a positive effect on companies' decision to disclose cyber security information, and that board independence and financial expertise have a positive impact on the amount of these disclosures.	Future research is expected to improve on the shortcomings of this research in examining the impact of board effectiveness on issues related to cyber security disclosures.
32	2023	[54]	Sensors	This research classifies and analyses common security compromises related to IoT layered architectures, including connectivity, communication, and management protocols.	Future research is expected to further develop the classification and analysis of common security intrusions related to IoT layered architectures, including connectivity, communication, and management protocols.
33	2023	[55]	Continuity & Resilience Review	The results of this article show that cybercrime can be mitigated by using CCMF (cybercrime mitigation framework) to detect, assess, analyse, evaluate and respond to cybercrime to enhance security in an organisation's evolving threat landscape.	The challenge researchers will face in the future, is to conduct research on the evolving organisational threat landscape including: vulnerabilities caused by the integration of various network nodes and, subsequently, factors that influence these vulnerabilities include inadequate threat intelligence gathering, lack of third-party audits and inadequate control mechanisms
34	2024	[56]	International Journal of Disclosure and Governance	The research qualitatively provides evidence that public companies are addressing cyber security-related issues, emphasising how the three lines of defence (internal audit, information technology	the results of this research can be developed qualitatively and quantitatively in the future to show evidence that public companies are addressing cyber

				(IT), and information security (IS)), can contribute to cyber security effectiveness.	security-related issues comprehensively.
35	2024	[57]	Journal of Information Systems	The research was able to find a relationship between cyber security risk and audit pricing	Future research is expected to improve on the shortcomings of this research in examining the relationship between cyber security risk and audit pricing.
36	2024	[58]	Journal of Information Systems	We found that audit firms that have experience with clients that experienced a cyber security breach, ceteris paribus, charge higher audit fees than clients that did not experience a breach.	future research could add other variables besides auditors' experience with their clients' cyber security incidents, to influence subsequent audits and help those clients reduce cyber security risks.

Source: personalized processed data, 2025

Based on Table 2, it can be elaborated that cyber security audits are generally immensely needed in ITG. Moreover, several studies previously stated above emphasize that it is highly recommended that the board of directors master cyber security audit, so that they are able to anticipate various impacts arising from violations and data leaks related to information technology governance.

In this section, it is explained the results of research and at the same time is given the comprehensive discussion. Results can be presented in figures, graphs, tables and others that make the reader understand easily.

CONCLUSIONS AND RECOMMENDATIONS

Cyber security audits and Information Technology Governance are two key components needed to maintain information security and manage information technology effectively. Integration between the two in a conceptual framework helps organizations identify, manage and mitigate cyber risks while maintaining alignment with business objectives. Building a solid understanding of this relationship is an important step for facing the increasingly complex cyber security challenges of today's digital era. Future studies are recommended to develop this research in terms of such as digging in-depth information with external partners about cyber security and ITG, increasing the depth of information between internal auditors and cyber security management. In addition, future research also needs to add several other variables, including variables to measure professional perceptions about information security, risk management variables to improve the effectiveness of information security management and ITG comprehensively. Internal auditor variable who is an expert plays a role as a substitute for the board of directors if there is no board of directors mastering cyber security auditing in ITG. Therefore, he relatively new cyber security audit themes can run dynamically according to developments in IoT and artificial intelligence (AI).

REFERENCES

[1] A. A. Ganie and S. Devi, "Emerging cyber threats in the digital age: trends and challenges," *Int.*

Res. J. Mod. Eng. Technol. Sci., vol. 05, no. 03, pp. 2542–2546, 2023, [Online]. Available: www.irjmets.com

[2] A. Calder and S. Watkins, *IT Governance: An international guide to data security and ISO27001/ISO27002*, 6th ed. London Philadelphia New Delhi: Kogan Page Limited, 2015.

[3] K. D. Jadhav, "The Role of cyber security audits in managing company systems and aplications," *Exp. Find.*, no. January, pp. 1–7, 2023, [Online]. Available: https://www.researchgate.net/publication/367559332_THE_ROLE_OF_CYBER_SECURITY_AUDITS

[4] S. Slapničar, T. Vuko, M. Čular, and M. Drašček, "Effectiveness of cybersecurity audit," *Int. J. Account. Inf. Syst.*, vol. 44, no. January 2021, pp. 1–21, 2022, doi: 10.1016/j.accinf.2021.100548.

[5] N. I. Jaafar and E. Jordan, "Information Technology Governance (ITG) practices and accountability of Information Technology (IT) projects - A case study in a Malaysian Government-Linked Company (GLC)," in *PACIS 2009 - 13th Pacific Asia Conference on Information Systems: IT Services in a Global Environment*, 2009, pp. 1–15.

[6] K. Al-Dosari and N. Fetais, "Risk-management framework and information-security systems for Small and Medium Enterprises (SMEs): A Meta-analysis approach," *Electron.*, vol. 12, no. 17, 2023, doi: 10.3390/electronics12173629.

[7] E. Haapamäki and J. Sihvonen, "Cybersecurity in accounting research," *Manag. Audit. J.*, vol. 34, no. 7, pp. 808–834, 2019, doi: 10.1108/MAJ-09-2018-2004.

[8] M. Antunes, M. Maximiano, and R. Gomes, "A Client-centered information security and cybersecurity auditing framework," *Appl. Sci.*, vol. 12, no. 9, 2022, doi: 10.3390/app12094102.

[9] M. Antunes, M. Maximiano, and R. Gomes, "A customizable web platform to manage standards compliance of information security and cybersecurity auditing," in *Procedia Computer Science*, 2021, vol. 196, pp. 36–43. doi: 10.1016/j.procs.2021.11.070.

[10] B. Azinheira, M. Antunes, M. Maximiano, and R. Gomes, "A methodology for mapping cybersecurity standards into governance guidelines for SME in Portugal," *Procedia Comput. Sci.*, vol. 219, no. 2021, pp. 121–128, 2023, doi: 10.1016/j.procs.2023.01.272.

[11] S. Slapničar, T. Vuko, M. Cular, and M. Drascek, "Effectiveness of cybersecurity audit," *Int. J. Account. Inf. Syst.*, vol. 44, no. 100548, pp. 1–21, 2022.

[12] J. Bouwens, "Auditors: their mindset and their decisions," *Maandbl. Voor Account. en Bedrijfsecon.*, vol. 90, no. 10, pp. 385–390, 2016, doi: 10.5117/mab.90.31181.

[13] G. Hardy, "X Coordinating IT governance-A new role for the IT strategy committee," *Inf. Syst. Control J.*, vol. 4, pp. 1–5, 2003.

[14] P. Best and S. Buckby, "Development of a board IT governance (ITG) review model," in *Accounting & Finance Association of Australia and New Zealand Conference (AFAANZ 2007)*, 2007, no. March, pp. 1–16. [Online]. Available: http://eprints.usq.edu.au/6031/

[15] S. Buckby, P. Best, and J. Stewart, "The Role of boards in reviewing Information Technology Governance (ITG) as part of organizational control environment assessments," in *Proceedings 2005 IT Governance International Conference*, 2005, pp. 1–15.

[16] G. J. Selig, *Implementing IT Governance: A practical guide to global best practices in IT Management*, 1st ed., no. December. 2008. [Online]. Available: https://books.google.es/books?hl=es&lr=&id=rdVEBAAAQBAJ&oi=fnd&pg=PR5&dq=implementing+it+governance+a+practical+guide+to+global+best+practices+in+it+management&ots=K_vhQQNhEl&sig=mw7_EdcxzSK4PHH4pfKv1xa7DGE

[17] S. Slapničar, M. Axelsen, I. Bongiovanni, and D. Stockdale, "A pathway model to five lines of accountability in cybersecurity governance," *Int. J. Account. Inf. Syst.*, vol. 51, no. August, 2023, doi: 10.1016/j.accinf.2023.100642.

[18] G. Lame, "Systematic literature reviews: An introduction," in *Proceedings of the International Conference on Engineering Design, ICED*, 2019, no. July, pp. 1633–1642. doi: 10.1017/dsi.2019.169.

[19] R. Handayani, E. Utami, and E. T. Luthfi, "Systematic literature review on auditing information technology risk management using the COBIT framework," *Prism. Sains*, vol. 11, no. 4, pp. 1028–1036, 2023, doi: 10.33394/j-ps.v11i4.8871.

[20] A. Trifu, E. Smîdu, D. O. Badea, E. Bulboacă, and V. Haralambie, "Applying the PRISMA method

for obtaining systematic reviews of occupational safety issues in literature search," in *MATEC Web of Conferences*, 2022, vol. 354, p. 00052. doi: 10.1051/matecconf/202235400052.
[21] S. Simamora, "Systematic literature review with the prisma method: the impact of blockchain technology on digital advertising," *M-Progress*, vol. 14, no. 1, 2024, doi: 10.35968/m-pu.v14i1.1182.
[22] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, no. n71, pp. 1–9, 2021, doi: 10.1136/bmj.n71.
[23] A. Liberati *et al.*, "The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration," *PLoS Med.*, vol. 6, no. 7, pp. 1–28, 2009, doi: 10.1371/journal.pmed.1000100.
[24] I. A. Moosa, "Publish or perish: Origin and perceived benefits," in *Publish or Perish*, 2018, pp. 1–17. doi: 10.4337/9781786434937.00007.
[25] J. Gabrielsson, "Corporate governance and entrepreneurship : current states and future directions," in *Handbook of Research on Corporate Governance and Entrepreneurship*, 2017, pp. 1–25.
[26] D. F. Al Husaeni and A. B. D. Nandiyanto, "Bibliometric using Vosviewer with Publish or Perish (using Google Scholar data): from step-by-step processing for users to the practical examples in the analysis of digital learning articles in pre and post Covid-19 pandemic," *ASEAN J. Sci. Eng.*, vol. 2, no. 1, pp. 19–46, 2022, doi: 10.17509/ajse.v2i1.37368.
[27] P. L. Bowen, M. Y. D. Cheung, and F. H. Rohde, "Enhancing IT governance practices: A model and case study of an organization's efforts," *Int. J. Account. Inf. Syst.*, vol. 8, no. 3, pp. 191–221, 2007, doi: 10.1016/j.accinf.2007.07.002.
[28] P. J. Steinbart, R. L. Raschke, G. Gal, and W. N. Dilla, "The relationship between internal audit and information security: An exploratory investigation," *Int. J. Account. Inf. Syst.*, vol. 13, no. 3, pp. 228–243, 2012, doi: 10.1016/j.accinf.2012.06.007.
[29] P. J. Steinbart, R. L. Raschke, G. Gal, and W. N. Dilla, "Information Security Professionals' Perceptions about the Relationship between the Information Security and Internal Audit Functions," *J. Inf. Syst.*, vol. 27, no. 2, pp. 65–86, 2013.
[30] B. Kuerbis and F. Badiei, "Mapping the cybersecurity institutional landscape," *Digit. Policy, Regul. Gov.* , vol. 19, no. 6, pp. 466–492, 2017, doi: 10.1108/DPRG-05-2017-0024.
[31] T. Stafford and S. Islam, "Information technology (it) integration and cybersecurity/security: The security savviness of board of directors," in *AMCIS 2017 - America's Conference on Information Systems: A Tradition of Innovation*, 2017, vol. 2017-Augus, pp. 1–5.
[32] M. van Eeten, "Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity," *Digit. Policy, Regul. Gov.* , vol. 19, no. 6, pp. 429–448, 2017, doi: 10.1108/DPRG-05-2017-0029.
[33] E. Amir, S. Levi, and T. Livne, "Do firms underreport information on cyber-attacks? Evidence from capital markets," *Rev. Account. Stud.*, vol. 23, no. 3, pp. 1177–1206, 2018, doi: 10.1007/s11142-018-9452-4.
[34] S. Bozkus Kahyaoglu and K. Caliyurt, "Cyber security assurance process from the internal audit perspective," *Manag. Audit. J.*, vol. 33, no. 4, pp. 360–376, 2018, doi: 10.1108/MAJ-02-2018-1804.
[35] M. S. Islam, N. Farah, and T. F. Stafford, "Factors associated with security/cybersecurity audit by internal audit function: An international study," *Manag. Audit. J.*, vol. 33, no. 4, pp. 377–409, 2018, doi: 10.1108/MAJ-07-2017-1595.
[36] T. Stafford, G. Deitz, and Y. Li, "The role of internal audit and user training in information security policy compliance," *Manag. Audit. J.*, vol. 33, no. 4, pp. 410–424, 2018, doi: 10.1108/MAJ-07-2017-1596.
[37] P. J. Steinbart, R. L. Raschke, G. Gal, and W. N. Dilla, "The influence of a good relationship between the internal audit and information security functions on information security outcomes," *Accounting, Organ. Soc.*, vol. 71, pp. 15–29, 2018, doi: 10.1016/j.aos.2018.04.005.
[38] B. von Solms and R. von Solms, "Cybersecurity and information security – what goes where?," *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 2–9, 2018, doi: 10.1108/ICS-04-2017-0025.
[39] F. Caron, "Obtaining reasonable assurance on cyber resilience," *Manag. Audit. J.*, vol. 36, no. 2, pp. 193–217, 2019, doi: 10.1108/MAJ-11-2017-1690.

[40] T. J. Smith, J. L. Higgs, and R. E. Pinsker, "Do auditors price breach risk in their audit fees?," *J. Inf. Syst.*, vol. 33, no. 2, pp. 177–204, 2019, doi: 10.2308/isys-52241.
[41] A. M. A. M. Al-Sartawi, "Information technology governance and cybersecurity at the board level," *Int. J. Crit. Infrastructures*, vol. 16, no. 2, pp. 150–161, 2020, doi: 10.1504/ijcis.2020.10029173.
[42] H. Li, W. G. No, and J. Efrim Boritz, "Are external auditors concerned about cyber incidents? Evidence from audit fees," *Audit. A J. Pract. Theory*, vol. 39, no. 1, pp. 151–171, 2020, doi: 10.2308/ajpt-52593.
[43] C. C. Hartmann and J. Carmenate, "Academic research on the role of corporate governance and it expertise in addressing cybersecurity breaches: Implications for practice, policy, and research," *Curr. Issues Audit.*, vol. 15, no. 2, pp. A9–A23, 2021, doi: 10.2308/CIIA-2020-034.
[44] T. Vuko, S. Slapničar, M. Čular, and M. Drašček, "Key drivers of cybersecurity audit effectiveness: the neo-institutional perspective," *SSRN Electron. J.*, no. October, 2021, doi: 10.2139/ssrn.3932177.
[45] S. Héroux and A. Fortin, "Board of directors' attributes and aspects of cybersecurity disclosure," *J. Manag. Gov.*, no. 0123456789, p. 10997, 2022, doi: 10.1007/s10997-022-09660-7.
[46] M. Malatji, A. L. Marnewick, and S. Von Solms, "Cybersecurity capabilities for critical infrastructure resilience," *Inf. Comput. Secur.*, vol. 30, no. 2, pp. 255–279, 2022, doi: 10.1108/ICS-06-2021-0091.
[47] C. Medoh and A. Telukdarie, "The Future of Cybersecurity: A System Dynamics Approach," *Procedia Comput. Sci.*, vol. 200, no. 2019, pp. 318–326, 2022, doi: 10.1016/j.procs.2022.01.230.
[48] R. Villalón-Fonseca, "The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity," *Comput. Secur.*, vol. 120, pp. 1–22, 2022, doi: 10.1016/j.cose.2022.102805.
[49] A. Fortin and S. Héroux, "Limited usefulness of firm-provided cybersecurity information in institutional investors' investment analysis," *Inf. Comput. Secur.*, vol. 31, no. 1, pp. 108–123, 2023, doi: 10.1108/ICS-07-2022-0122.
[50] H. M. Melaku, "A Dynamic and Adaptive Cybersecurity Governance Framework," *J. Cybersecurity Priv.*, vol. 3, no. 3, pp. 327–350, 2023, doi: 10.3390/jcp3030017.
[51] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience," *Sensors*, vol. 23, no. 7273, pp. 1–27, 2023, doi: 10.3390/s23167273.
[52] K. Shaheen and A. H. Zolait, "The impacts of the cyber-trust program on the cybersecurity maturity of government entities in the Kingdom of Bahrain," *Inf. Comput. Secur.*, vol. 31, no. 5, pp. 529–544, 2023, doi: 10.1108/ICS-06-2022-0108.
[53] N. Smaili, C. Radu, and A. Khalili, "Board effectiveness and cybersecurity disclosure," *J. Manag. Gov.*, vol. 27, no. 4, pp. 1049–1071, 2023, doi: 10.1007/s10997-022-09637-6.
[54] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," *Sensors*, vol. 23, no. 4117, pp. 1–46, 2023, doi: 10.1080/19361610.2021.1962677.
[55] A. Yeboah-Ofori and F. A. Opoku-Boateng, "Mitigating cybercrimes in an evolving organizational landscape," *Contin. Resil. Rev.*, vol. 5, no. 1, pp. 53–78, 2023, doi: 10.1108/crr-09-2022-0017.
[56] S. Héroux and A. Fortin, "How the three lines of defense can contribute to public firms' cybersecurity effectiveness," *Int. J. Discl. Gov.*, p. 2, 2024, doi: 10.1057/s41310-024-00226-7.
[57] W. Jiang, "Cybersecurity Risk and Audit Pricing—A Machine Learning-Based Analysis," *J. Inf. Syst.*, vol. 38, no. 1, pp. 91–117, 2024, doi: 10.2308/ISYS-2023-019.
[58] H. Li, Z. Sun, and F. Huang, "The Impact of Audit Office Cybersecurity Experience on Nonbreach Client's Audit Fees and Cybersecurity Risks," *J. Inf. Syst.*, vol. 38, no. 1, pp. 177–206, 2024, doi: 10.2308/ISYS-2023-014.