The 1st International Student Conference on Economics and Business Excellence (ISCEBE) 2024
e-ISSN: xxxx-xxxx/Vol. 1 No.1 (2024)

TWO DECADES OF INFORMATION SECURITY AUDIT RESEARCH: A META-ANALYSIS REVIEW OF METHODS AND TECHNIQUES IN INFORMATION SECURITY AUDITING

Galant Victory[1)], Asniati Bahari[2)]
[1-2)]Accounting Department, Universitas Andalas, Indonesia
Corresponding author: asniati@eb.unand.ac.id

Abstract

Cybercrime has been on the increase and continues to affect a wide range of organizations, bringing both direct and indirect costs. Information security audits have evolved as a means of safeguarding an organization's value and key data assets through the appraisal of policies, standards, and security measures that have been put in place. The current study sets out to trace and interpret the scholarly developments in the area of information security audits in the last twenty years, that is, within the period of 2004-2024, with particular interest on techniques and methods used in Indonesia and other places in the world. Taking advantage of meta analysis particularly the PRISMA approach, this study collected data from qualitative sources in the scopus and google databases and was able to identify 23 articles from reputable sources. Such articles were thereafter mapped by means of VOSViewer to assess the popular sub topics of the articles and future research niches. The research noted an increase in the number of research output after the year 2021, although there are still some sub topics such as "risk", "control" and "auditors" that require attention. There is need to create an audit framework that incorporates the changing technologies in order to enhance the shared responsibility between the industry and the academia in the quest of improving information security. The implications of these findings are intended to advance the work done in the area of information security audits both in theory and practice.

Keywords: Information Security Audit, Adaptive Audit Framework, Cybersecurity Framework, Bayesian Inference-Based Method, PRISMA Methodology

Introduction

Cybercrime can have significant economic impacts on organizations, both directly and indirectly. Direct impacts include asset misuse, theft of personal information, disruption of online operations, and legal costs arising from resolving consumer claims related to damages. Indirect economic impacts occur when disclosures of information security risks, governance policies, and security breaches significantly affect the organization's reputation and value (Steinbart et al., 2018). In the current digital era, ensuring the security of information system assets has become a top priority for organizations to protect against malicious attacks such as cybercrime and data breaches, which are continually increasing. Since information and information systems play a central role in organizational operations, the focus on and importance of information security has grown substantially (Alraja et al., 2023; Khando et al., 2021). Studies evidence the quality of systems and information has a significant effect on organizational performance (Bahari & Mahmud, 2018). A survey conducted by the European Confederation of Institutes of Internal Auditors (ECIIA) involving 799 Chief Audit Executives (CAEs) identified cybersecurity and data security as the top business risks for 2024, with projections indicating that these will remain the highest risks through 2027 (ECIIA, 2023).

In its simplest concept, information security can be defined as the effort to protect information systems and data from intrusions, malicious software, and unauthorized use. Beyond this, information security poses various risks to businesses, including risks of legal violations related to information, reputational damage due to data breaches, system failures that disrupt business operations, and becoming a target of political actions that could interfere with commercial activitie (Laybats & Tredinnick, 2016).

The maintenance and enhancement of an organization's reputation are closely linked to how information is managed. Adequate security is a critical aspect of information and information systems management. Systems must be designed with security integrated into the existing security architecture. Security architecture is not a product but rather a model that defines services such as authentication, authorization, auditing, and intrusion detection, which must be addressed by the technology. This model enables a comparison of the applications in such a way that it is possible to be sure that the different applications implement similar security services, thus, the applications are built such that they fit into one security model (Otero, 2019).

Establishing security policies and guidelines along with adhering to the organizational information assurance goals and security policies is one of the crucial measures to ensure information security in organizations (Stafford et al., 2018). In order for these policies to be effective, there should be efforts towards undertaking verification, validation and information security audits to ascertain that the implementation is well organized. Internal control and processes of information security are periodically assessed by independent internal audit providing a good framework for the management of IT risks and control (Steinbart et al., 2015).

Information security audits represent a new dimension in security practices, aiming to protect an organization's critical information assets. The audit process seeks to gather evidence regarding the security policies and their effectiveness in safeguarding the integrity, confidentiality, accessibility, and availability of data (Islam et al., 2018). Information security audits are mainly about how an organization ensures that the users of its technology adhere and practice security standards (Stafford et al., 2018). Such audits measure how well an organization is able to defend its valuable or critical assets as well as measure the effectiveness of information security management, and the need for enhancements in standard operating practices (Pereira & Santos, 2010). As such, investigating the patterns of academic interest in the research of information security audits is important as it can have great effects on private businesses, government agencies and the general population. Understanding changes within a particular area will only be possible through routine evaluations of literature within that specific area. Reviews of this sort help researchers to discern such things as new developments, new perspectives and the changing emphases of appropriate research, thus enabling them to ensure that their studies are relevant to the current needs or challenges (Snyder, 2019; Palvia et al., 2017).

The main focus of this study is to carry out identification and analysis of academic scholarly work concerning information security audits with particular emphasis to the methods and techniques employed in such audits with respect to Indonesia and other countries. The research evaluates the overall status of studies, compares trends in Indonesia with those abroad over the past 20 years, and identifies future research needs. This kind of research is aimed at providing, or enhancing development of theory of information security audits and also its application in practice.

Methods

The present study integrates a meta-analytical approach, specifically those stated in the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta Analyses) framework, which encouages researchers of systematic reviews and meta-analyses to provide full and clear details concerning the methods implemented (Liberati et al., 2009). Meta-analysis refers to a statistical technique within systematic reviews that integrates the findings of included studies (Moher et al., 2010).

1. Search Terms

Scopus and Google Scholar databases were used to collect the data and the range of publication years was set between 2004 and 2024. The approach used a typology of article's title, abstract and keywords searching for the phrases "information security audit" with the aid of Publish or Perish application. Such keywords included: "information security audit," "information system security audit," "IT security audit," and "cybersecurity audit". These keywords were also translated into Bahasa Indonesia with a view to establish what works emanated from the Indonesian territory.

2. Selection Process

Prior to the selection process, a search was conducted using keywords relevant to information security audits, and all retrieved data were included without initial filtering. The first selection step involved screening articles based on format to exclude books, reports, theses, organizational manuscripts, and media articles. Subsequently, the titles and abstracts of articles meeting the criteria were reviewed to ensure their relevance to information security audits. Papers containing the term "audit" in the title but unrelated to information security audits were excluded. Duplicate articles from the Scopus and Google Scholar databases were also filtered out.

The next step involved selecting articles based on Scopus and SINTA indexing. Only articles from reputable journals indexed in Scopus or SINTA (levels 1–4) were accepted. Articles from conference proceedings were included only if indexed in Scopus. The final step was to select articles relevant to the topic of methods, tools, and techniques used in information security audits. The review process was started by considering the titles and abstracts of the articles; when these were not provided or were not enough, entire texts were read.

e-ISSN: xxxx-xxxx/Vol. 1 No.1 (2024)

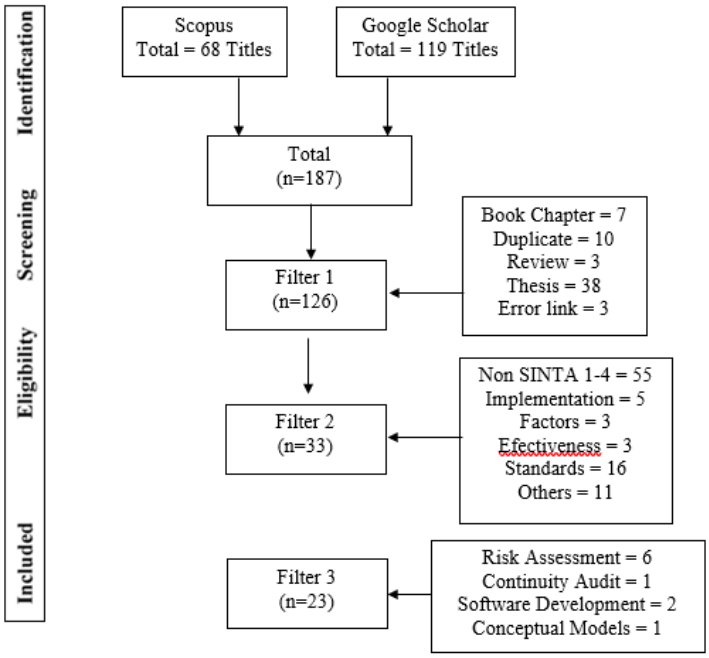
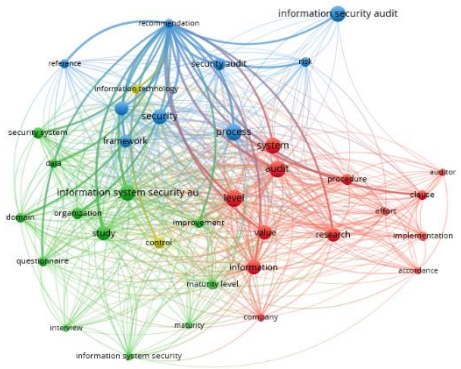


Figure 1
Literature Review Method

3. Research Mapping

The collected articles were then mapped using VOSviewer software. VOSviewer is a computer application designed for the purpose of creating, building and visualizing bibliometric maps. This application allows for the use of clustering models in mapping and layout models. Such mapped information can be presented and visualized in different forms including overlay and density visualizations, among others. VOSviewer serves for bibliometric data analysis, for visualization of large amount of data, and for representation of intellectual and developing aspects of a defined area of research (van Eck & Waltman, 2010; Verma & Gustafsson, 2020). The articles were subsequently classified based on subtopics to identify popular research areas and methodologies.



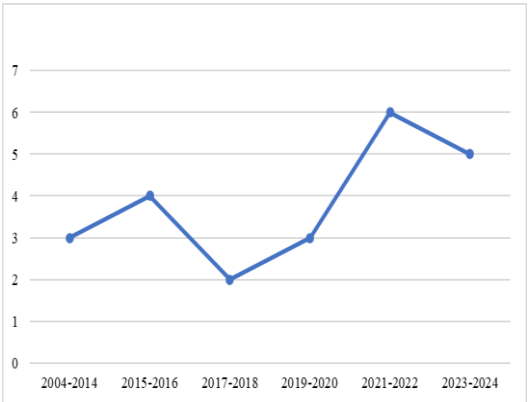


Figure 2 visualizes the keyword mapping results of the articles. The mapping is divided into four clusters, represented by four different colors, with three dominant clusters. In VOSviewer, clusters are defined as groups of items displayed on the map, with each item representing a term. Colors are used by VOSviewer to indicate the clusters to which the items are assigned (van Eck & Waltman, 2010).

The items "level" and "process" are the most frequently occurring terms, with an occurrence of 13–14. The term "audit" appears 12 times, followed by "information system security audit," "system," and "information security audit," each appearing 11 times. This indicates that research in the field of information security audits, particularly on topics such as methods and techniques, remains limited, as evidenced by occurrences below 20. Terms such as "risk," "control," and "auditor," also appear infrequently, suggesting that research on information security audits with these subtopics is still underexplored.

The distribution of articles over time is illustrated in Figure 2, covering the interval from before 2014 to 2023. As shown, there is an observable trend of increasing research on information security audit methods beginning in 2021, despite fluctuations in other years. Considering the progression of articles over time and the sample of research studies, this trend suggests that research on information security audit methods has been gaining increasing attention from academics and researchers. Consequently, this topic remains an area of interest for further investigation.

Results and Discussions

The results and discussion section presents the results, analysis of literature review data according to the predetermined research objectives, and discussion of topics related to the results.

Tabel 1. Information Security Audit Method & Techniques

No	Method & Techniques	Study
1	Bayesian Inference-Based Methods	(Ndife et al., 2022); (Satoh & Samejima, 2019)
2	Open Source Intelligence (OSINT)	(Bryushinin et al., 2022); (Melshiyan & Dushkin, 2022)
3	Frameworks and Models for Cybersecurity Audits	(Sabillon & Barr, 2024); (Sabillon et al., 2017); (Sabillon et al., 2024)
4	Blockchain in Audits	(König et al., 2023)
5	Fuzzy Cognitive Modelling	(Rytov et al., 2017); (Lakhno et al., 2021)
6	Simulation Modelling	(Turner, 2022); (Shao et al., 2015)
7	XML Technologies	(Golyash et al., 2011)
8	Methodology, Ontologies and Expert Systems	(Atymtayeva et al., 2012)
9	Threat Feature Extraction	(Zakaria et al., 2019)
10	Risk Analysis and Comparative Studies	(Alimzhanova et al., 2022);(Livshitz et al., 2016)
11	Quantitative Analysis & Framework	(Satoh, 2012); (Jiang, 2024); (Deaver-Vazquez et al., 2024)
12	Failure Modes and Effects Analysis	(Wijaya & Hakim, 2020)

1. Bayesian Inference-Based Methods

From the literature review, it is evident that there exist two articles that discuss Information Security Audits in relation to the Bayesian approach. The use of the Bayesian approach in the information security audit is aimed at spotting on audit risk and keywords which assist auditors in detecting the presence of a risk, not observed previously, through the use of dependent probabilities to access the relationship between the terms in the audit report. Borrowing from the bag of words model, past audit reports provide useful words for estimating the likelihood of risk keywords utilizing Bayes' Theorem while adjusting for the occurrence of certain words in prospective reports with respect to the audited organization. Risk keywords with the highest probabilities are given to auditors with supporting evidence which includes associated words and the risk pertaining targets, which are self-updated as new risks emerge. As a consequence, this practice has been addressed to improve risk determination with up to 20% for novice auditors and with 12% for experienced ones, but it has shortcomings in advance in determining risks that are very specific to some organizations. This technique also shows how probability approaches can enhance the efficacy and effectiveness of risk management in information security audits that are text oriented (Satoh & Samejima, 2019).

Ndife et al. (2022) implemented Bayesian Neural Networks providing results regarding Threat detection in Smart Grids to address the uncertainty in the problem. One limitation is that this model not only gives the probability of attack type, but also provides attack probabilities which are most likely to be the outputs. To obtain uncertainty in estimating the posterior distribution, it used Variational inference where KL Divergence between the prior di-stribution and the posterior one is minimized while dropout performed regularization, to prevent overfitting and simulate sample distributions. This method helps in reducing the uncertainty estimates, detecting new (zero-day) attacks and enhances multiclass classification. In the applications of smart grids, to address the problem of threat recognition spatiotemporal features were used and SGtechNet reduced the model size up to 25% with no accuracy lost and hence, an efficient and lightweight solution was developed. The bayesian approach offers better flexibility and can be used in

several protective scenarios including IoT traffic analysis and malware detection as every decision made is based on the most reliable probabilistic analytics.

2. Open Source Intelligence (OSINT)

Bryushinin et al. (2022); Melshiyan & Dushkin (2022) discuss the use of Open Source Intelligence (OSINT) to detect vulnerabilities in an organization's information and telecommunications networks during an information security audit. The OSINT method is the expansion of the scope of an audit where information that is not conventional audit material; such as, unindexed files with personal data or classified technologies that are difficult to obtain by normal search techniques are established. In this article, several strategies of automated information gathering from OS include the use of a computer and the language Python within the context of supporting penetration testing. Organizational information, employees, and the software and hardware appear as several highlighted vectors of information collection. Also such software that is set to perform open-source information analysis automatically and to generate information in an appropriate and visual format to support the audit work. This OSINT method broadens the scope of the usual key audit techniques and fills in the gaps that are always taken for granted in most audits when information leakage channels are not visible; hence foresees recommendations that warrant more drastic changes in the organization's information security.

3. Frameworks and Models for Cybersecurity Audits

Sabillon et al. (2017) present an advanced and flexible cybersecurity audit approach regarding the context of growing sophistication of the threats and challenges in the cyber environment. The model unifies elements of ordinary IT audits together with the components of InfoSec and Cyber Assurance operating in a slightly different philosophy of adapting to progressing threats. The model pursues the adoption of advanced technologies like AI, machine learning or big data analytics for more rapid and timely detection of threats. Additionally, Sabillon & Barr (2024) place a highlight on the need to sustain cybersecurity culture in the organization through training and awareness as well as continuously looking to improve the need for assessment in light of new threats. There is also a risk-based approach which focuses on risk and controls which are of high impact, however, the use of third parties will also add value to this audit. In general this model intends to enhance security confidence and practice by integrating technical, policy and risk management in a holistic fashion.

Sabillon et al. (2024) proposes a comprehensive cybersecurity audit model, which has been validated through empirical analysis. The model includes audit of internal system vulnerabilities and risk management procedures; evaluation of institutional adherence to the relevant security laws; formulation of the cyber security policies and plans for each institution; application of the risk based audit to reduce the impact of the changing information security risks. It is anticipated that this audit model will be adopted by higher education institutions in Canada and will provide an adaptable and more reliable means of addressing the cyber security audit challenges of the increasingly sophisticated security threats.

4. Blockchain & XML Technologies in Audits

König et al. (2023) propose the challenges faced in the practice of conducting blockchain-supported distributed security audit of information and articulate the existing security audit challenges related to the distributed security audit model. With the aid of the blockchain architecture, the audits can be performed on a decentralized basis which could improve the level of trust and transparency amongst parties involved in detailed networks such as supply chains. Golyash et al. (2011) highlights the use of XML technologies like XBRL or the Semantic Web in improving the audit process since it allows for the establishment of a definite structure as a format that allows the easier management and examination of security data. The audit process has four levels and comprises of expert examination, targeting the increase and improvement of risk management more efficiently through XML technologies in the areas of data processing and retrieval.

5. Fuzzy Cognitive Modelling

Fuzzy Cognitive Modeling (FCM) is applicable in information security audits of information portals of regional executive authorities, as a means for dealing with uncertainty and complexity in information systems. FCM provides the ability to explain relations among the components of the system, such as policies, technologies, and people, to identify risks and weak points. Furthermore, FCM helps auditors comprehend and evaluate potential weaknesses within systems as well as, the integrated effects of multiple threats, thereby enhancing information security effectiveness. This strategy incorporates more accurate evaluations in places where uncertainty is high, and dynamism is the order of the day (Rytov et al., 2017).

The assurance of information security becomes easier when the information is audited under the Information Security Audit method based on neural-fuzzy system which uses a neural network technology and fuzzy sets to evaluate the level of security of information objects. While Fuzzy sets provide some type of IS assessment ambiguity through the use of more non rigid values. Neural networks generate correct and detailed decisions based on the information on complicated risk data and its patterns with regard to the

systems. Hence the integration of both enables a relatively more comprehensive and dynamic evaluation of information security determining frameworks that combine standardized indicators and expert opinion based on the features of IS management and the organization of IO. This system not just enhances the effectiveness of audits but also facilitates the administration of IO, cuts down the costs and enhances efficiency of the business processes (Lakhno et al., 2021).

6. Simulation Modelling

The Next-Generation Audit Management Environment (NGAME) is an application utilizing the Process Mining approach to perform cybersecurity audits, specifically in dealing with auditor-audited party asymmetries. Within this framework, Process Mining is applied to control and measure the processes within information systems with respect to the established security requirements, for example, a need-to-have access approval policy (Turner, 2022).

Shao et al. (2015) focus on a solution for a cluster monitoring system that aims to ensure cyber security through server cluster, where each server node has a daemon to gather performance metrics and processes performance metrics to cut as well as detects faults in the system clusters for the real time monitoring and man management of servers. The system was built to have active security measures for possible threats and technical glitches that would require reporting for system audits and further assuring better overall protection and performance from the side of information security.

7. Methodology, Ontologies and Expert Systems

The aim of creating automated software systems for information security audits is to decrease the expenses, speed up the procedures, and increase the overall quality of the audit process while meeting international standards of information security. The experts proposed methodology incorporates sophisticated expert systems based on fuzzy logic which assists in coping with uncertainties and imprecisions inherent in multifaceted decision-making contexts during the audit trial. In this system, Ontology is deployed to structure knowledge about the various central focus of security audits such as risks, weaknesses, and relevant security measures. Such ontology is utilized to create the building blocks around which models for the expert system are constructed, so that it can rapidly assess risk levels and issue recommendations with precision and speed. In this way, it speeds up and decreases how much human input is needed in the audit process. This methodology and ontology are aimed towards a much more efficient, effective and high-quality expert system for the redesigning of the security audit process (Atymtayeva et al., 2012).

8. Threat Feature Extraction

The Feature Extraction and Selection Method in cyberattack and threat profiling is aimed at the determination and the selection of the crucial features within the data collected with respect to the cyber attacks or the threats during the audit. Feature extraction deals with obtaining certain relevant features from primary sources of data including logs, network traffic indicators, targets and sources of attacks or features defining anomaly patterns. After features are extracted, those features that are the most informative among them are being selected in order to enhance the accuracy while minimizing the amount of data which in turn improves processing power requirements. Considering a smaller number of the most informative features enables timelier and more accurate threat detection capabilities. This approach is broadly consistent with the increasing trends towards attack and threat profiling based on knowledge of certain attack features and behavior patterns. In the light of mounting complexities of cyber security violations in audit processes, this approach helps the auditors develop a more structured and evidence based approach in the threat detection, evaluation and response while at the same time enhancing the design of appropriate counter measure plans (Zakaria et al., 2019).

9. Risk Analysis and Comparative Studies

Alimzhanova et al. (2022) investigates a threat and vulnerability analysis model which focuses on evaluating in detail the information security needs of an organization and recording the results. This model is designed to avoid unnecessary expenses related to subjective risk evaluations, to guarantee that security practices are embedded into all phases of the information systems development and use processes, and to schedule risk evaluation so as to save effort, reduce mistakes and cut dependence on specialist knowledge. The research further examines other types of risk assessment problems and software tools to propose a sound model on how to calculate risk on sound and objective. This improves the efficiency of managing information security risks by making the processes and evaluation of risks uniform, and standard procedures are followed at all times.

Livshitz et al. (2016) proposes a combined method that integrated approach which relies on the combination of standard methods for real-time auditing and on continuous monitoring of a system based on the requirements of ISO 27001 and ISO 19011 standards with the addition of IT security metrics. This

approach, as illustrated, increases the response time for corrective actions of Information Security Management System (ISMS), which results in better detection and handling of zero-day attacks.

10. Quantitative Analysis & Framework

Satoh (2012) provides a methodology for determining the duration required to conduct an information security audit. It uses 21 audit cases already carried out taking into account different characteristics that determine the extent of the work like the category of the audit, work done, extent of audit undertaken, how well the auditor is and for how big the organization is. Such modeling describes how long the time needed in doing each of those work could be done through regression analysis techniques. Such analysis has also helped to ascertain how long the certain tasks in a specific project could be performed, with the reports indicating a possible error of between 7.5% and about 7% within the accepted figure as proposed by Project Management Body of Knowledge (PMBOK). This method allows for a more precise estimation of audit time, facilitating resource planning and management in information security audits.

Jiang (2024) suggests that, to measure the potential cybersecurity risk of organizations, one could utilize machine learning algorithms integrated with features that include such variables as the willingness to report cybersecurity shortcomings, level of information technology best practices governance, the level of dependency on external factors such as financial analysts, auditors, etc, and other organization metrics. This algorithm succeeds logistic regression models in terms of risk measurement, is more effective in the assessment of contemporary industries that are more susceptible to cyber attacks, and even forecasts the incidences of data breaches and the utilization of the cybersecurity insurance cover by corporations. Deaver-Vazquez et al. (2024) discusses the significance of risk measurements during cybersecurity audit processes focusing on decision-making, which helps the organizations' survivability. They also present a risk measurement system where complexity barriers have been removed such that auditors can compute risks in a traditional way by estimating proportions without having to use complicated software tools.

11. Failure Modes and Effects Analysis

Wijaya & Hakim (2020) articulates the necessity of formulating audit tools that are directed towards risk assessment of the systems using such analytical approaches as Failure Modes and Effects Analysis (FMEA) to determine potential failure points. Audit criteria are based on control measures that guarantee the operational effectiveness of information security systems and the audit tools in question are expected to be used for continual improvement and system breakdown minimization.

Conclusion

This article discusses the development of information security audit research over the past two decades (2004–2024), focusing on the methods and techniques employed. Utilizing a meta-analysis approach applying the PRISMA approach, the research gathers information from two databases, Scopus and Google scholar, obtaining 23 relevant articles. Out of these 23 articles a total of 12 sub topics concerning the methods and techniques used in information security audits have been identified and entail the approaches and tools that were designed to improve the efficacy of information security audit practices. In general, the primary outcomes of the investigation emphasize on the adaptation of existing information security range of audits in the context of advancing technology. To augment the level of information security in organizations, the need of further enhance partnership between industry and academia is dire. The result and discussion section bring out terms such as "level", "process", and "audit" as common whereas terms such as "risk", "controls", "auditors" are most of the time broken dow and are seldom the subject of major coverage thus meaning that there is much scope for consideration. Moreover, it has been outlined that there has to be a new audit model which is comprehensive in its approach or design rather combing the core elements of traditional IT audit and the Industry best practices on Information Security and Cyber Security Assurance. New technologies, including artificial intelligence (AI), machine learning, and big data analytics, are also viewed as crucial in enhancing threat detection in real-time as well as in developing an internal cyber security culture within an organization. All in all, while the inquiry about information security audits has developed and is still developing, other issues, especially those regarding risk, controls, and auditors' effectiveness in protecting the integrity of information systems, need to be explored further.

References

Alimzhanova, Z., Tleubergen, A., Zhunusbayeva, S., & Nazarbayev, D. (2022). Comparative Analysis of Risk Assessment During an Enterprise Information Security Audit. *2022 International Conference on Smart Information Systems and Technologies (SIST)*, 1–6. https://doi.org/10.1109/SIST54437.2022.9945804

Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers & Security*, *129*, 103208. https://doi.org/10.1016/j.cose.2023.103208

Atymtayeva, L. B., Bortsova, G. K., Inoue, A., & Kozhakhmet, K. T. (2012). Methodology and ontology of expert system for information security audit. *The 6th International Conference on Soft Computing and Intelligent Systems, and The 13th International Symposium on Advanced Intelligence Systems*, 238–243. https://doi.org/10.1109/SCIS-ISIS.2012.6505287

Bahari, A., & Mahmud, R. (2018). Impact of System Quality, Information Quality and Service Quality on Performance. *34th Annual Computer Security Applications Conference*. http://repo.unand.ac.id/5029/1/Asniati%20Bahari-Roslinah%20Mahmud.pdf

Bryushinin, A. O., Dushkin, A. V., & Melshiyan, M. A. (2022). Automation of the Information Collection Process by Osint Methods for Penetration Testing During Information Security Audit. *2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, 242–246. https://doi.org/10.1109/ElConRus54750.2022.9755812

Deaver-Vazquez, C., Taylor, E., Rowley, D., & Langis, B. (2024). BEYOND PASS/FAIL: DEVELOPING A QUANTITATIVE FRAMEWORK FOR CYBERSECURITY AUDITS. *EDPACS*, *69*(4), 1–6. https://doi.org/10.1080/07366981.2024.2340848

ECIIA. (2023). *Risk in focus 2024. Hot topics for internal auditors*. https://www.eciia.eu/wp-content/uploads/2023/09/CIIA-Risk-in-Focus-2024_final-web.pdf

Golyash, I., Sachenko, S., & Rippa, S. (2011). Improving the information security audit of enterprise using XML technologies. *Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems*, 795–798. https://doi.org/10.1109/IDAACS.2011.6072879

Islam, Md. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function. *Managerial Auditing Journal*, *33*(4), 377–409. https://doi.org/10.1108/MAJ-07-2017-1595

Jiang, W. (2024). Cybersecurity Risk and Audit Pricing—A Machine Learning-Based Analysis. *Journal of Information Systems*, *38*(1), 91–117. https://doi.org/10.2308/ISYS-2023-019

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

König, L., Pirker, M., Geyer, H., Feldmann, M., Tjoa, S., & Kieseberg, P. (2023). *DISA - A Blockchain-Based Distributed Information Security Audit* (pp. 27–34). https://doi.org/10.1007/978-3-031-48316-5_4

Lakhno, V., Akhmetov, B., Chubaievskyi, V., Desiatko, A., Palaguta, K., Blozva, A., & Chasnovskyi, Y. (2021). *Information Security Audit Method Based on the Use of a Neuro-Fuzzy System* (pp. 171–184). https://doi.org/10.1007/978-3-030-90318-3_17

Laybats, C., & Tredinnick, L. (2016). Information security. *Business Information Review*, *33*(2), 76–80. https://doi.org/10.1177/0266382116653061

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., Clarke, M., Devereaux, P. J., Kleijnen, J., & Moher, D. (2009). The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration. *PLoS Medicine*, *6*(7), e1000100. https://doi.org/10.1371/journal.pmed.1000100

Livshitz, I. I., Yurkin, D. V., & Minyaev, A. A. (2016). *Formation of the Instantaneous Information Security Audit Concept* (pp. 314–324). https://doi.org/10.1007/978-3-319-51917-3_28

Melshiyan, M. A., & Dushkin, A. V. (2022). Information Security Audit Using Open Source Intelligence Methods. *2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, 379–382. https://doi.org/10.1109/ElConRus54750.2022.9755530

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2010). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *International Journal of Surgery*, *8*(5), 336–341. https://doi.org/10.1016/j.ijsu.2010.02.007

Ndife, A. N., Mensin, Y., Rakwichian, W., & Muneesawang, P. (2022). Cyber-Security Audit for Smart Grid Networks: An Optimized Detection Technique Based on Bayesian Deep Learning. *Journal of Internet Services and Information Security*, *12*(2), 95–114. https://doi.org/10.22667/JISIS.2022.05.31.095

Otero, A. R. (2019). *Information Technology Control and Audit* (5th ed.). CRC Press Taylor & Francis Group.

Palvia, P., Patrick Y.K., C., Daneshvar Kakhki, M., Ghoshal, T., Uppala, V., & Wang, W. (2017). A decade plus long introspection of research published in Information & Management. *Information & Management*, *54*(2), 218–227. https://doi.org/10.1016/j.im.2016.06.006

Pereira, T., & Santos, H. M. D. (2010). An audit framework to support information system security management. *International Journal of Electronic Security and Digital Forensics*, *3*(3), 265. https://doi.org/10.1504/IJESDF.2010.038288

Rytov, M. Y., Leksikov, E. V, Sakalo, V. I., & Kovalev, P. A. (2017). The Use of Fuzzy Cognitive Modelling to Manage Information Security Audit of Information Portals of Regional Executive Authorities. *Journal of Physics: Conference Series*, *803*, 012131. https://doi.org/10.1088/1742-6596/803/1/012131

Sabillon, R., & Barr, M. (2024). Planning and Conducting Cybersecurity Audits to Assess the Effectiveness of Controls. *2024 IEEE International Systems Conference (SysCon)*, 1–6. https://doi.org/10.1109/SysCon61195.2024.10553588

Sabillon, R., Higuera, J. R. B., Cano, J., Higuera, J. B., & Montalvo, J. A. S. (2024). Assessing the Effectiveness of Cyber Domain Controls When Conducting Cybersecurity Audits: Insights from Higher Education Institutions in Canada. *Electronics*, *13*(16), 3257. https://doi.org/10.3390/electronics13163257

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). *2017 International Conference on Information Systems and Computer Science (INCISCOS)*, 253–259. https://doi.org/10.1109/INCISCOS.2017.20

Satoh, N. (2012). A Labor Times Estimation Method for the Information Security Audit by Quantitative Analysis I and Regressive Analysis. *IEEJ Transactions on Electronics, Information and Systems*, *132*(11), 1855–1859. https://doi.org/10.1541/ieejeiss.132.1855

Satoh, N., & Samejima, M. (2019). Risk words suggestion for information security audit by Bayesian inference. *Electronics and Communications in Japan*, *102*(1), 42–48. https://doi.org/10.1002/ecj.12133

Shao, Z., Zeng, G., Gong, R., Li, Y., & Zhang, K. (2015). Design and implementation of cluster monitoring on information security audit system. *2015 6th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 718–721. https://doi.org/10.1109/ICSESS.2015.7339158

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal*, *33*(4), 410–424. https://doi.org/10.1108/MAJ-07-2017-1596

Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. N. (2015). The Influence of Internal Audit on Information System Effectiveness: Perceptions of Internal Auditors. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2685943

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*, 15–29. https://doi.org/10.1016/j.aos.2018.04.005

Turner, R. C. (2022). Process Mining for Asymmetric Cybersecurity Audit. *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, 293–298. https://doi.org/10.1109/CSR54599.2022.9850298

van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, *84*(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

Verma, S., & Gustafsson, A. (2020). Investigating the emerging COVID-19 research trends in the field of business and management: A bibliometric analysis approach. *Journal of Business Research*, *118*, 253–261. https://doi.org/10.1016/j.jbusres.2020.06.057

Wijaya, R. A. P., & Hakim, A. R. (2020). DESIGN OF INTERNAL AUDIT TOOLS FOR INFORMATION SECURITY SYSTEMS IN ORGANIZATION XYZ. *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK)*, *7*(3), 435–442. https://doi.org/10.25126/jtiik.202071940

Zakaria, K. N., Zainal, A., Othman, S. H., & Kassim, M. N. (2019). Feature Extraction and Selection Method of Cyber-Attack and Threat Profiling in Cybersecurity Audit. *2019 International Conference on Cybersecurity (ICoCSec)*, 1–6. https://doi.org/10.1109/ICoCSec47621.2019.8970786