Cybersecurity Audit and IT Risk Management

Andreanov, Renny Maisyarah

Abstract

Cybersecurity and IT risk management have become paramount for organizations in the face of growing cyber threats. As digital technologies and interconnected systems evolve, organizations must implement robust frameworks to safeguard sensitive data and ensure business continuity. This systematic literature review (SLR) examines 14 scholarly articles published between 2019 and 2025, focusing on the role of cybersecurity audits, IT risk management frameworks, leadership influence, and the impact of prior cyberattack disclosures on cybersecurity practices. The review addresses three central research questions: (1) How do cybersecurity audit frameworks contribute to improving IT risk management practices across various sectors? (2) What is the role of leadership, such as CEO power and audit committees, in shaping cybersecurity audit and IT risk management strategies? (3) How does the disclosure of prior cyberattacks impact the effectiveness of cybersecurity audits and IT risk management reporting? The findings suggest that cybersecurity audit frameworks, such as NIST and blockchain-based models, play a critical role in identifying and managing cybersecurity risks. Leadership involvement, especially from CEOs and audit committees, significantly shapes the effectiveness of cybersecurity strategies. Furthermore, disclosing previous cyberattacks fosters transparency, enhances investor confidence, and improves cybersecurity audits and reporting. This review provides comprehensive insights into the evolving role of cybersecurity audit and IT risk management frameworks, offering theoretical and practical recommendations for organizations aiming to enhance their cybersecurity resilience.

***Keywords**:* Cybersecurity Audit, IT Risk Management, NIST Framework, Leadership Influence, Cyberattack Disclosure.

Andreanov
Accounting Magister Program, Universitas Pembangunan Panca Budi, Indonesia
e-mail: andreanov15@gmail.com

Renny Maisyarah
e-mail: rennymaisyarah@dosen.pancabudi.ac.id

Introduction

Cybersecurity has become one of the most critical concerns for organizations across various industries, particularly with the increasing dependency on digital technologies and interconnected systems. As cyber threats continue to evolve, organizations are tasked with implementing robust cybersecurity risk management frameworks to protect sensitive data, ensure business continuity, and maintain stakeholder trust. The importance of effective cybersecurity risk management is further emphasized by the growing number of cyberattacks that disrupt operations and compromise data integrity [1]; [2].

This systematic literature review (SLR) aims to explore the evolving role of cybersecurity risk management frameworks, highlighting their application, effectiveness, and impact across diverse sectors such as healthcare, smart cities, financial institutions, and auditing practices. Drawing on a comprehensive selection of 14 scholarly articles published between 2019 and 2025, this review examines the diverse independent and dependent variables influencing cybersecurity practices. These include the role of internal auditors, CEO power, audit committees, investor perceptions, and the adoption of frameworks such as the NIST Risk Management Framework, among others [13]; [5].

The reviewed studies contribute valuable insights into how different frameworks and strategies enhance the resilience of organizations to cybersecurity risks. From blockchain identity management systems in healthcare IoT to the role of internal audit strategies in financial institutions, this review provides a thorough analysis of the mechanisms and practices shaping cybersecurity governance [6]. Additionally, it delves into the implications of improved reporting and independent assurance in strengthening organizational cybersecurity postures, and the impact these practices have on investor confidence and regulatory compliance [8]; [7]. By synthesizing these findings, this review aims to offer a comprehensive understanding of the current state of cybersecurity risk management, offering both theoretical insights and practical recommendations for organizations striving to enhance their cybersecurity resilience.

The growing complexity and sophistication of cyber threats have made it increasingly important for organizations to adapt their cybersecurity strategies continuously. With the expansion of digital transformation and the rise of smart cities, the integration of advanced technologies like blockchain and AI has significantly reshaped how cybersecurity risks are managed. As such, this review emphasizes the need for organizations to not only focus on the technical aspects of cybersecurity but also to consider the governance frameworks, organizational culture, and leadership roles that impact risk management [10]; [13], By analyzing these diverse frameworks and their effectiveness, this review provides an in-depth look at how organizations can build a proactive cybersecurity posture that is adaptable to evolving threats while ensuring compliance with emerging global standards.

This paper presents a Systematic Literature Review (SLR) of 14 peer-reviewed articles published between 2019 and 2025, Cybersecurity Risk Management, Cybersecurity Auditing, Internal, Auditing, Risk Assessment, and Independent Assurance. The review seeks to answer the following research questions:

1. How do cybersecurity audit frameworks contribute to improving IT risk management practices across various sectors?
2. What is the role of leadership, such as CEO power and audit committees, in shaping cybersecurity audit and IT risk management strategies?

3. How does the disclosure of prior cyberattacks impact the effectiveness of cybersecurity audits and IT risk management reporting?

Literature Review

The field of cybersecurity audit and IT risk management is rapidly evolving due to the increasing complexity of cyber threats and the growing reliance on digital technologies. As organizations continue to face sophisticated cyberattacks, robust auditing practices and effective IT risk management frameworks are becoming essential to safeguarding sensitive data and ensuring business continuity. This section synthesizes insights from 14 studies on cybersecurity auditing and IT risk management, focusing on the role of auditing frameworks, risk management strategies, and leadership in improving organizational resilience to cyber threats.

2.1 Cybersecurity Risk Management Frameworks

Several studies explore the development and application of cybersecurity risk management frameworks that are essential for mitigating IT risks [1], proposed a blockchain-based identity management framework for Health IoT (BC-IdM) to enhance data security and privacy. This framework is particularly relevant in sectors like healthcare, where data confidentiality is crucial. Chaudhuri and Bozkus Kahyaoglu [2], examined the application of the NIST Risk Management Framework in smart cities to address cybersecurity risks arising from interconnected city systems. The use of such frameworks enables organizations to manage and reduce cybersecurity risks systematically, ensuring that they can adapt to emerging threats and vulnerabilities.

2.2 The Role of Leadership in Cybersecurity and IT Risk Management

Leadership plays a critical role in shaping cybersecurity practices and IT risk management strategies. Al-Shaer et al., [12] investigated the influence of CEO power and audit committees on cybersecurity risk management, emphasizing the role of top executives in prioritizing cybersecurity initiatives. Their research suggests that leadership involvement is crucial for aligning cybersecurity goals with overall business strategies. Similarly, [13], highlighted the impact of CEO power in driving cybersecurity efforts and ensuring the effective implementation of risk management strategies. Effective governance from leadership ensures that cybersecurity remains a key focus, with adequate resources allocated to risk mitigation .

2.3 Cybersecurity Auditing and Internal Control Mechanisms

Cybersecurity auditing is an integral part of managing IT risks and ensuring compliance with security standards. Wertheim [5], stressed the importance of audits in identifying vulnerabilities and assessing the effectiveness of cybersecurity controls. Internal audits help detect weaknesses in systems and provide organizations with the insights needed to improve their security posture. Usman et al. [9] explored how the characteristics of internal auditors impact the effectiveness of cybersecurity risk assessments, particularly in financial organizations. Their findings suggest that experienced auditors who understand both the technical and business aspects of cybersecurity are better equipped to identify and mitigate risks. Furthermore, [6]. proposed a client-centered auditing approach, emphasizing the importance of tailoring audits to meet the specific needs and risks of different organizations .

2.4 Investor Perception and Cybersecurity Reporting

The quality of cybersecurity reporting significantly influences investor confidence. Yang et al. (2020) examined the impact of cybersecurity risk management reporting frameworks on investor perceptions. Transparent and comprehensive reporting builds trust with investors, making them more confident in the organization's ability to manage cyber risks.

Similarly, [13], analyzed how the disclosure of prior cyberattacks affects organizational transparency and investor confidence. Their study showed that organizations that disclose previous security incidents and demonstrate their commitment to improving cybersecurity practices are more likely to earn the trust of investors, which is crucial for long-term business success.

2.5 Cybersecurity in the Context of Emerging Technologies

Emerging technologies such as blockchain and artificial intelligence are reshaping the cybersecurity landscape, bringing new challenges and opportunities for IT risk management. Giuca et al, [10] conducted a survey of various cybersecurity risk management frameworks, focusing on how these technologies are integrated into existing risk management strategies. They found that as organizations adopt new technologies, they must update their risk management frameworks to account for the unique risks these technologies introduce, such as data integrity issues and advanced cyberattacks .

2.6 Enhancing Audit Assurance

Sánchez-García et al. [8] developed guidelines for performing cybersecurity risk audits, emphasizing the importance of structured methodologies and continuous monitoring to improve cybersecurity assurance. Their work highlights that audits should not be a one-time event but rather an ongoing process that adapts to new risks and threats. Lois et al. [7] further discussed the procedural contributions of internal auditing in strengthening cybersecurity practices. They argued that effective audits are essential for ensuring that cybersecurity controls remain up to date and that any weaknesses in security systems are promptly addressed

Research Methodology

The systematic literature review (SLR) methodology employed in this study aims to synthesize and analyze existing research on **Cybersecurity Audit and IT Risk Management** by examining 14 scholarly articles published between 2019 and 2025. The SLR methodology follows a structured, systematic approach to identify, evaluate, and synthesize relevant studies to draw meaningful insights. This methodology ensures that the review is comprehensive, unbiased, and transparent in its findings.

3.1 Research Objectives

The primary objective of this SLR is to:

a. Examine the role of cybersecurity audits in IT risk management practices.
b. Assess the impact of cybersecurity frameworks on organizational risk management.
c. Investigate the influence of leadership, reporting, and auditing practices in managing cybersecurity risks.

3.2 Selection Criteria

The inclusion and exclusion criteria for selecting relevant studies were established to ensure the relevance and quality of the selected journals. The criteria are as follows:

Inclusion Criteria**:**

a. Peer-reviewed journal articles published from 2019 to 2025.
b. Studies focusing on cybersecurity auditing, IT risk management, internal audit strategies, or frameworks.
c. Articles that provide empirical data, case studies, or conceptual frameworks related to cybersecurity audits and IT risk management.
d. Studies published in high-impact journals in the fields of information systems, cybersecurity, and business management (Q1-Q4, as indexed in Google Scholar).
e. Only journals indexed in reputable databases (such as Scopus, Web of Science) were considered to ensure the quality of the articles.

Exclusion Criteria**:**

a. Articles not focused on cybersecurity or IT risk management.
b. Studies that do not discuss cybersecurity audits or relevant auditing frameworks.
c. Non-peer-reviewed articles or articles not published in reputable journals.

3.3 Data Extraction

Data extraction involved collecting relevant information from the selected articles to answer the research questions. The key data points extracted from each article included:

a. Authors and Year of Publication: To track the chronological development of the field.
b. Study Focus: A brief description of the primary focus of each article (e.g., cybersecurity auditing frameworks, internal audit strategies, leadership in cybersecurity).
c. Research Methodology: Whether the study used qualitative, quantitative, or mixed methods.
d. Key Findings and Contributions: Summarizing the main findings, including insights into the role of cybersecurity audits, frameworks, risk management strategies, and leadership influence on IT risk management.

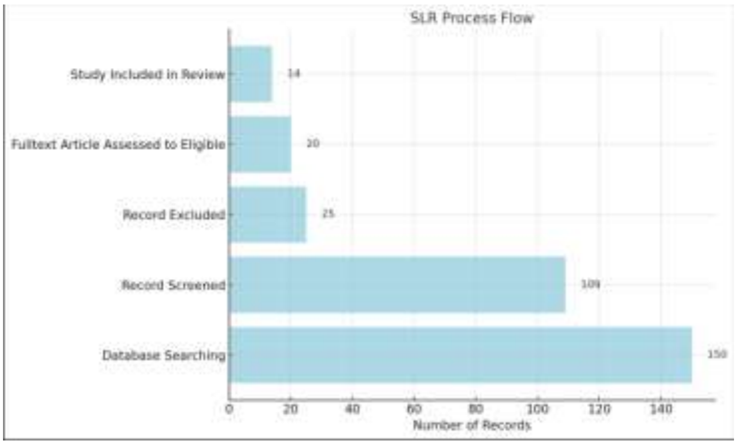
3.4 Synthesis and Analysis

After data extraction, the findings from the selected studies were synthesized and analyzed to identify:

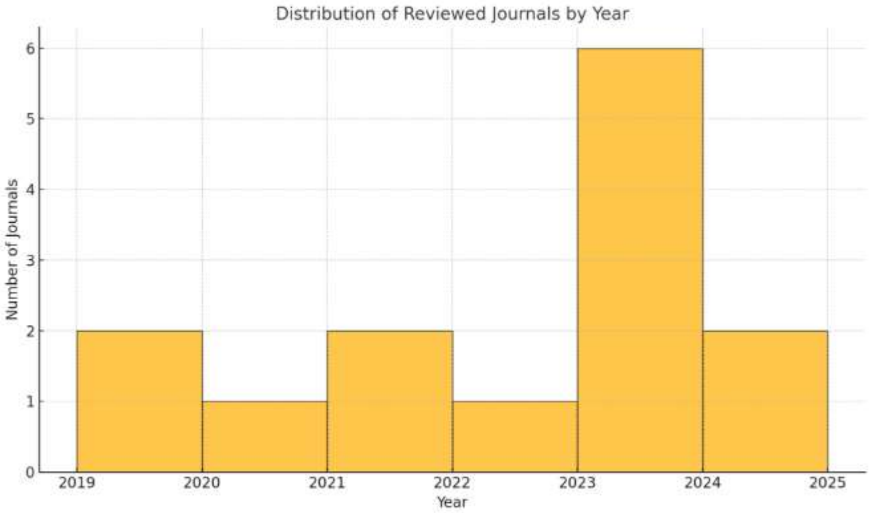
a. Common Themes: Identifying recurring themes such as the effectiveness of cybersecurity auditing frameworks, the role of internal audits, and the influence of leadership on risk management strategies.
b. Methodological Approaches: Analyzing the methodologies used in the studies to assess the strengths and limitations of different approaches.
c. Gaps in the Literature: Identifying areas where further research is needed, such as the integration of emerging technologies (e.g., AI, blockchain) into cybersecurity audits and risk management frameworks.

Results and Discussion

Data items extracted from each article were summarized as follows: year of publication, authors, country and research setting, type of data and methodological approach, key research variables, "Smart contract auditing", "Blockchain-based audit systems", "Automated auditing with smart contracts". The stages of the systematic literature review are comprehensively illustrated in Figure 1.



These findings are further structured in the PRISMA flow diagram (Figure 1) and expanded upon in the following subsections.



In addition, the 14 chosen papers underwent a qualitative synthesis, as indicated in Table1.

No	Year	Author	Title	Country & Sample	Purpose
1	2023	Alamri, B.; Crowley, K.; Richardson, I.	Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT	Ireland, 106 studies reviewed (focusing on Health IoT, Blockchain, and Identity Management)	Untuk mengembangkan dan mengusulkan kerangka manajemen risiko keamanan untuk sistem identitas berbasis blockchain (BC-IdM) di Health IoT (HIoT), yang bertujuan untuk meningkatkan keamanan dan privasi data pengguna di sistem ini.
2	2023	Chaudhuri, A., & Bozkus Kahyaoglu, S.	Cybersecurity assurance in smart cities: A risk management perspective	Global (focus on smart cities globally)	To address the growing cybersecurity risks in smart cities by proposing a risk management framework using NIST's Risk Management Framework for smart city councils to ensure effective cybersecurity assurance.
3	2019	Frank, M. L., Grenier, J. H., & Pyzoha, J. S.	How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance	USA, 68 companies across various sectors	Untuk mengkaji bagaimana pengungkapan serangan siber sebelumnya mempengaruhi efektivitas pelaporan manajemen risiko siber dan jaminan independen dalam organisasi.
4	2020	Yang, L., Lau, L., & Gan, H.	Investors' perceptions of the cybersecurity risk management reporting framework	International (focus on investors from various regions)	Untuk menyelidiki persepsi para investor terhadap kerangka pelaporan manajemen risiko keamanan siber

					yang digunakan dalam laporan perusahaan yang terdaftar.
5	2019	Wertheim, S.	Auditing for cybersecurity risk	USA, auditors, cybersecurity professionals	Untuk menjelaskan pentingnya audit dalam manajemen risiko keamanan siber dan bagaimana audit dapat membantu mendeteksi serta mengurangi ancaman terhadap sistem informasi organisasi.
6	2022	Antunes, M., Maximiano, M., & Gomes, R.	A client-centered information security and cybersecurity auditing framework	International (various client-centered industries)	Untuk mengembangkan kerangka audit keamanan informasi dan keamanan siber yang berfokus pada kebutuhan dan ekspektasi klien dalam rangka meningkatkan efektivitas audit di berbagai sektor industri.
7	2021	Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D.	Internal auditing and cyber security: audit role and procedural contribution	International (focus on internal audit and cybersecurity practices)	Untuk mengeksplorasi peran audit internal dalam pengelolaan risiko siber dan kontribusinya dalam prosedur-prosedur keamanan di organisasi.
8	2023	Sánchez-García, I. D., Gilabert, T. S. F., & Calvo-Manzano, J. A.	CRAG: A Guideline to Perform a Cybersecurity Risk Audits	International (focus on cybersecurity audit guidelines)	To provide a structured approach for conducting cybersecurity risk audits, specifically designed for improving cybersecurity assurance across various sectors.
9	2023	Usman, A., Ahmad, A. C., & Abdulmalik, S. O.	The role of internal auditors' characteristics in cybersecurity risk assessment in financial-based business organisations: A conceptual review	International (focus on financial-based organizations)	To review the role of internal auditors' characteristics in assessing cybersecurity risks in financial-based business organizations.
10	2021	Giuca, O., Popescu, T. M., Popescu, A. M., Prostean, G., & Popescu, D. E.	A survey of cybersecurity risk management frameworks	International (survey of multiple frameworks)	To explore various cybersecurity risk management frameworks, with a focus on their application in different industries and technologies, particularly in the context of emerging technologies like blockchain
11	2025	Ferreira, L. V. A., Alves, C. A. D. M., Peotta de Melo, L., & Nunes, R. R.	Internal Audit Strategies for Assessing Cybersecurity Controls in the Brazilian Financial Institutions	Brazil, Financial Institutions	To explore the role of internal audit strategies in evaluating cybersecurity controls within the Brazilian financial sector.
12	2025	Al-Shaer, H., Albitar, K., Derouiche, I., & Hussainey, K.	The Role of CEO Power and Audit Committees in	International (focused on financial organizations)	To examine how CEO power and audit committees influence the effectiveness of

			Cybersecurity Risk Management		cybersecurity risk management in organizations.
13	2023	Frank, M. L., Grenier, J. H., Pyzoha, J. S., & Zielinski, N. B.	Implications of enhanced cybersecurity risk management reporting and independent assurance	USA, 50 financial organizations and auditors	To analyze the implications of improved cybersecurity risk management reporting and independent assurance on organizational practices and investor confidence.
14	2023	Frank, M. L., Grenier, J. H., Pyzoha, J. S., & Zielinski, N. B.	Implications of enhanced cybersecurity risk management reporting and independent assurance	USA, 50 financial organizations and auditors	To analyze the implications of improved cybersecurity risk management reporting and independent assurance on organizational practices and investor confidence

Here is the table with **Independent Variables (IV)** added for each study from 1 to 14 based on the context:

No	**Year**	**Author**	**Title**	**Dependent Variable (DV)**	**Independent Variable (IV)**
1	2023	Alamri, B.; Crowley, K.; Richardson, I.	Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT	Cybersecurity Risk Management Framework (BC-IdM in Health IoT)	Blockchain Identity Management, Health IoT Systems, Data Privacy Concerns, Cybersecurity Risks
2	2023	Chaudhuri, A., & Bozkus Kahyaoglu, S.	Cybersecurity assurance in smart cities: A risk management perspective	Cybersecurity Assurance in Smart Cities	Interdependent Systems in Smart Cities, Risk Management, Cyberattack Incidents, NIST Risk Management Framework
3	2019	Frank, M. L., Grenier, J. H., & Pyzoha, J. S.	How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance	Efficacy of Cybersecurity Risk Management Reporting	Disclosure of Prior Cyberattack, Independent Assurance, Reporting Practices
4	2014	Coronado, A. J., & Wong, T. L.	Healthcare cybersecurity risk management: Keys to an effective plan	Healthcare Cybersecurity Risk Management Plan	Technology Adoption, Organizational Preparedness, Risk Assessment in Healthcare, Data Protection Regulations
5	2020	Yang, L., Lau, L., & Gan, H.	Investors' perceptions of the cybersecurity risk management reporting framework	Investors' Perceptions of Cybersecurity Reporting Framework	Reporting Framework, Investor Confidence, Organizational Cybersecurity Practices, Risk Management Practices
6	2019	Wertheim, S.	Auditing for cybersecurity risk	Effectiveness of Cybersecurity Risk Audits	Internal Audit Strategies, Cybersecurity Controls, Organizational Cybersecurity

					Practices, Audit Procedures
7	2022	Antunes, M., Maximiano, M., & Gomes, R.	A client-centered information security and cybersecurity auditing framework	Information Security and Cybersecurity Auditing Effectiveness	Client-Centered Audit Approach, Auditing Framework, Cybersecurity Risk Assessment, Client Needs
8	2021	Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D.	Internal auditing and cyber security: audit role and procedural contribution	Internal Audit Role in Cybersecurity Risk Management	Internal Audit Strategies, Cybersecurity Procedures, Organizational Cybersecurity Risk Culture
9	2023	Sánchez-García, I. D., Gilabert, T. S. F., & Calvo-Manzano, J. A.	CRAG: A Guideline to Perform a Cybersecurity Risk Audits	Cybersecurity Risk Audit Guidelines	Cybersecurity Risk Audits, Risk Management Frameworks, Assessment Methodologies
10	2023	Usman, A., Ahmad, A. C., & Abdulmalik, S. O.	The role of internal auditors characteristics in cybersecurity risk assessment in financial-based business organisations: A conceptual review	Cybersecurity Risk Assessment in Financial-Based Organizations	Internal Auditor Characteristics, Organizational Cybersecurity Practices, Risk Assessment Models
11	2021	Giuca, O., Popescu, T. M., Popescu, A. M., Prostean, G., & Popescu, D. E.	A survey of cybersecurity risk management frameworks	Cybersecurity Risk Management Frameworks	Cybersecurity Risk Frameworks, Industry Application, Emerging Technologies, Regulatory Compliance
12	2025	Ferreira, L. V. A., Alves, C. A. D. M., Peotta de Melo, L., & Nunes, R. R.	Internal Audit Strategies for Assessing Cybersecurity Controls in the Brazilian Financial Institutions	Cybersecurity Control Assessment in Financial Institutions	Internal Audit Strategies, Cybersecurity Control Frameworks, Risk Management Practices in Brazilian Financial Sector
13	2025	Al-Shaer, H., Albitar, K., Derouiche, I., & Hussainey, K.	The Role of CEO Power and Audit Committees in Cybersecurity Risk Management	Effectiveness of Cybersecurity Risk Management	CEO Power, Audit Committee Role, Corporate Governance, Risk Management Frameworks
14	2023	Frank, M. L., Grenier, J. H., Pyzoha, J. S., & Zielinski, N. B.	Implications of enhanced cybersecurity risk management reporting and independent assurance	Enhanced Cybersecurity Risk Management Reporting	Cybersecurity Reporting Practices, Independent Assurance, Enhanced Reporting Strategies, Organizational Transparency

4.1 Summary of the Impact

Here is the table with a summary of the impact of independent variables (IV) on dependent variables (DV).

No	Dependent Variable Group	Dependent Variable (DV)	Independent Variables (IV)	Summary of Impact
1	Cybersecurity Risk Management	Cybersecurity Risk Management Framework in Health IoT	Blockchain Identity Management, Health IoT Systems, Data Privacy Concerns, Cybersecurity Risks	Blockchain-based Identity Management and Health IoT Systems improve cybersecurity by enhancing privacy, security, and data control.
2	Cybersecurity Assurance	Cybersecurity Assurance in Smart Cities	Interdependent Systems in Smart Cities, Risk Management, Cyberattack Incidents, NIST Risk Management Framework	Effective risk management and NIST Framework reduce cybersecurity threats and enhance assurance in interdependent smart city systems.
3	Cybersecurity Reporting Effectiveness	Efficacy of Cybersecurity Risk Management Reporting	Disclosure of Prior Cyberattack, Independent Assurance, Reporting Practices	Disclosure of past cyberattacks improves the clarity and effectiveness of cybersecurity reporting, boosting confidence in organizational transparency.
4	Cybersecurity Risk Management Plan	Healthcare Cybersecurity Risk Management Plan	Technology Adoption, Organizational Preparedness, Risk Assessment in Healthcare, Data Protection Regulations	A robust cybersecurity risk management plan in healthcare is driven by technology readiness and adherence to data protection regulations.
5	Investor Perception	Investors' Perceptions of Cybersecurity Reporting Framework	Reporting Framework, Investor Confidence, Organizational Cybersecurity Practices, Risk Management Practices	A clear and comprehensive cybersecurity reporting framework increases investor confidence and perception of risk management efficacy.
6	Cybersecurity Audit Effectiveness	Effectiveness of Cybersecurity Risk Audits	Internal Audit Strategies, Cybersecurity Controls, Organizational Cybersecurity Practices, Audit Procedures	Strong internal audits and effective cybersecurity controls improve the detection and mitigation of cybersecurity risks in organizations.
7	Cybersecurity Auditing	Information Security and Cybersecurity Auditing Effectiveness	Client-Centered Audit Approach, Auditing Framework, Cybersecurity Risk Assessment, Client Needs	A client-centered audit framework enhances the effectiveness of cybersecurity audits by addressing specific client needs and risks.
8	Cybersecurity Risk Management Culture	Internal Audit Role in Cybersecurity Risk Management	Internal Audit Strategies, Cybersecurity Procedures, Organizational Cybersecurity Risk Culture	Internal audit strategies influence organizational culture, improving risk management and fostering a more proactive cybersecurity stance.
9	Cybersecurity Risk Auditing	Cybersecurity Risk Audit Guidelines	Cybersecurity Risk Audits, Risk Management Frameworks, Assessment Methodologies	Cybersecurity risk audit guidelines based on effective frameworks and methodologies lead to better risk assessment and mitigation strategies.
10	Cybersecurity Risk Assessment	Cybersecurity Risk Assessment in Financial-Based Organizations	Internal Auditor Characteristics, Organizational Cybersecurity Practices, Risk Assessment Models	Internal auditors' characteristics directly affect the quality and accuracy of cybersecurity risk assessments in financial organizations.

11	Framework Implementation	Cybersecurity Risk Management Frameworks	Cybersecurity Risk Frameworks, Industry Application, Emerging Technologies, Regulatory Compliance	A structured and adaptable framework enhances the effectiveness of cybersecurity risk management across various industries and sectors.
12	Cybersecurity Control Assessment	Cybersecurity Control Assessment in Financial Institutions	Internal Audit Strategies, Cybersecurity Control Frameworks, Risk Management Practices in Brazilian Financial Sector	Audit strategies and control frameworks strengthen the assessment and management of cybersecurity risks in financial institutions.
13	Cybersecurity Risk Management Role	Effectiveness of Cybersecurity Risk Management	CEO Power, Audit Committee Role, Corporate Governance, Risk Management Frameworks	CEO power and audit committee involvement significantly influence the effectiveness of cybersecurity risk management in organizations.
14	Cybersecurity Risk Reporting	Enhanced Cybersecurity Risk Management Reporting	Cybersecurity Reporting Practices, Independent Assurance, Enhanced Reporting Strategies, Organizational Transparency	Enhanced reporting practices and independent assurance improve the transparency, accuracy, and reliability of cybersecurity risk management reporting.

The findings are discussed within the context of the selected studies, focusing on how cybersecurity audit frameworks contribute to IT risk management practices, the role of leadership in shaping strategies, and the impact of prior cyberattack disclosures on the effectiveness of reporting.

1. How do cybersecurity audit frameworks contribute to improving IT risk management practices across various sectors?

Cybersecurity audit frameworks play a crucial role in enhancing IT risk management practices by providing structured methodologies for identifying, evaluating, and mitigating cybersecurity risks. Studies such as those by [1], and [2], emphasize the importance of adopting standardized frameworks like the NIST Risk Management Framework to assess vulnerabilities and establish risk management practices. These frameworks enable organizations across sectors—such as healthcare, smart cities, and financial institutions—to systematically approach cybersecurity risk, ensuring that risks are adequately identified, controlled, and reported.

In healthcare, [1], introduced the blockchain identity management framework (BC-IdM) for Health IoT, which provides secure, decentralized identity management to protect sensitive patient data from cyber threats. This framework contributes significantly to IT risk management by ensuring the confidentiality and integrity of healthcare information systems, ultimately enhancing trust and security in the sector.

In the context of smart cities, [2], demonstrated that cybersecurity risks in interconnected urban systems require a robust, adaptive risk management approach. Their research advocated for a comprehensive application of NIST's framework, which helps identify risks arising from system interdependencies. The integration of cybersecurity audits into these frameworks allows cities to not only assess vulnerabilities but also create a dynamic risk management strategy that adapts to evolving technological landscapes.

2. What is the role of leadership, such as CEO power and audit committees, in shaping cybersecurity audit and IT risk management strategies?

Leadership plays a pivotal role in shaping the strategies for cybersecurity audits and IT risk management. The studies by [12] and [13], emphasize that CEO power and audit committees significantly influence the allocation of resources, the prioritization of cybersecurity initiatives, and the overall commitment to risk management practices. These leadership dynamics are essential for ensuring that cybersecurity becomes a key strategic focus rather than being relegated to a technical issue.

Al-Shaer et al. [12] argued that CEOs with strong authority and influence over organizational decisions are more likely to champion cybersecurity efforts and allocate sufficient resources to manage IT risks. In contrast, organizations with weaker CEO involvement in cybersecurity decision-making often struggle to implement comprehensive risk management frameworks. Similarly, audit committees play an integral role in ensuring that cybersecurity audits are properly conducted and that risk management strategies align with the organization's broader goals. The presence of a strong audit committee facilitates the oversight of cybersecurity initiatives, ensuring they are continuously updated and aligned with industry standards.

Frank et al. [13], highlighted the importance of CEO involvement in cybersecurity, noting that organizations with actively engaged CEOs in risk management efforts tend to exhibit stronger cybersecurity frameworks. CEOs set the tone for the organization's cybersecurity posture, guiding the integration of cybersecurity audits into the overall risk management strategy. Therefore, effective leadership, especially from the CEO and audit committees, is fundamental in ensuring that cybersecurity audits are conducted rigorously, and IT risk management strategies are continuously refined to address emerging threats.

3. How does the disclosure of prior cyberattacks impact the effectiveness of cybersecurity audits and IT risk management reporting?

The disclosure of prior cyberattacks plays a critical role in enhancing the effectiveness of cybersecurity audits and improving IT risk management reporting. Frank et al. [13], found that organizations that disclose past cyberattacks foster transparency and demonstrate a commitment to addressing cybersecurity vulnerabilities. This transparency builds trust with stakeholders, including investors and customers, and provides an opportunity for the organization to highlight the measures it has taken to mitigate future risks.

The act of disclosing prior incidents allows cybersecurity audits to focus on areas that were previously vulnerable, providing an opportunity for organizations to improve their security posture. By assessing past breaches, audit teams can develop more effective risk management strategies and recommend necessary improvements to organizational security protocols. For example, after a cyberattack, audits can analyze the effectiveness of existing security measures and assess whether changes are needed to prevent similar attacks in the future.

Conclusion

The findings from the reviewed studies emphasize the vital role that cybersecurity audit frameworks play in enhancing IT risk management practices across various sectors. Frameworks like NIST and blockchain-based models provide structured methodologies that help organizations identify, assess, and mitigate cybersecurity risks. In healthcare, the blockchain identity management framework ensures data security, while in smart cities, the NIST framework addresses risks arising from interconnected systems. These frameworks enable organizations to adapt to evolving cyber threats and integrate continuous improvement in their risk management practices.

Leadership, particularly CEO power and the involvement of audit committees, is crucial in shaping effective cybersecurity audit and IT risk management strategies. Studies reveal that CEOs who actively prioritize cybersecurity and engage in risk management decisions foster stronger, more proactive cybersecurity efforts. Additionally, audit committees ensure proper oversight of cybersecurity initiatives, aligning them with organizational goals and ensuring their effectiveness. Strong leadership is therefore essential in establishing a robust cybersecurity culture and ensuring that necessary resources are allocated to IT risk management.

The disclosure of prior cyberattacks enhances the effectiveness of cybersecurity audits and IT risk management reporting. By openly sharing information about past incidents, organizations demonstrate transparency and build trust with stakeholders, including investors and customers. This disclosure allows cybersecurity audits to focus on previously vulnerable areas and improve security measures. Furthermore, it contributes to more accurate and insightful IT risk management reporting, aligning with corporate governance best practices and fostering long-term organizational resilience to cyber threats.

References

[1] Alamri, B., Crowley, K., & Richardson, I. (2022). Cybersecurity risk management framework for blockchain identity management systems in health IoT. Sensors, 23(1), 218.De Andrés, J., & Lorca, P. (2021). On the impact of smart contracts on auditing. *International Journal of Digital Accounting Research*, *21*.

[2] Chaudhuri, A., & Bozkus Kahyaoglu, S. (2023). Cybersecurity assurance in smart cities: A risk management perspective. *Edpacs*, *67*(4), 1-22.

[3] Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. *Journal of Information Systems*, *33*(3), 183-200.

[4] Yang, L., Lau, L., & Gan, H. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. *International Journal of Accounting & Information Management*, *28*(1), 167-183.

[5] Wertheim, S. (2019). Auditing for cybersecurity risk. *The CPA Journal*, *89*(6), 68-71.

[6] Antunes, M., Maximiano, M., & Gomes, R. (2022). A client-centered information security and cybersecurity auditing framework. *Applied Sciences*, *12*(9), 4102.

[7] Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: audit role and procedural contribution. *International Journal of Managerial and Financial Accounting*, *13*(1), 25-47.

[8] Sánchez-García, I. D., Gilabert, T. S. F., & Calvo-Manzano, J. A. (2023, November). CRAG: A Guideline to Perform a Cybersecurity Risk Audits. In *International Congress of Telematics and Computing* (pp. 517-532). Cham: Springer Nature Switzerland.

[9] Usman, A., Ahmad, A. C., & Abdulmalik, S. O. (2023). The role of internal auditors characteristics in cybersecurity risk assessment in financial-based business organisations: A conceptual review. *International Journal of Professional Business Review: Int. J. Prof. Bus. Rev.*, *8*(8), 32.

[10] Giuca, O., Popescu, T. M., Popescu, A. M., Prostean, G., & Popescu, D. E. (2021). A survey of cybersecurity risk management frameworks. In *Soft Computing Applications: Proceedings of the 8th International Workshop Soft Computing Applications (SOFA 2018), Vol. I 8* (pp. 240-272). Springer International Publishing.

[11] Ferreira, L. V. A., Alves, C. A. D. M., Peotta de Melo, L., & Nunes, R. R. (2025). Internal Audit Strategies for Assessing Cybersecurity Controls in the Brazilian Financial Institutions. *Applied Sciences*, *15*(10), 5715.

[12] Al-Shaer, H., Albitar, K., Derouiche, I., & Hussainey, K. (2025). The Role of CEO Power and Audit Committees in Cybersecurity Risk Management. *The International Journal of Accounting*, 2542004.

[13] Frank, M. L., Grenier, J. H., Pyzoha, J. S., & Zielinski, N. B. (2023). Implications of enhanced cybersecurity risk management reporting and independent assurance. *Current Issues in Auditing*, *17*(1), P11-P18.

[14] Calderon, T. G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. *International Journal of Auditing*, *25*(1), 24-39.