Indonesian Journal of Law and Economics Review

Vol. 21 No. 1 (2026): February
DOI: 10.21070/ijler.v21i1.1523

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Indonesian Journal of Law and Economics Review
Vol. 21 No. 1 (2026): February
DOI: 10.21070/ijler.v21i1.1523

Table Of Contents

Journal Cover 1
Author[s] Statement 3
Editorial Team 4
Article information 5
Check this article update (crossmark) 5
Check this article impact 5
Cite this article 5
Title page 6
Article Title 6
Author information 6
Abstract 6
Article content 7

Indonesian Journal of Law and Economics Review
Vol. 21 No. 1 (2026): February
DOI: 10.21070/ijler.v21i1.1523

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Indonesian Journal of Law and Economics Review
Vol. 21 No. 1 (2026): February
DOI: 10.21070/ijler.v21i1.1523

EDITORIAL TEAM

Indonesian Journal of Law and Economics Review

Vol. 21 No. 1 (2026): February
DOI: 10.21070/ijler.v21i1.1523

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

(*) Time for indexing process is various, depends on indexing database platform

Indonesian Journal of Law and Economics Review

Vol. 21 No. 1 (2026): February
DOI: 10.21070/ijler.v21i1.1523

Integrating the Accounting Function into Cyber Risk Governance: A Proposed Organizational Framework to Strengthen Financial Information Protection in the Public Sector: Mengintegrasikan Fungsi Akuntansi ke dalam Tata Kelola Risiko Siber: Usulan Kerangka Kerja Organisasi untuk Memperkuat Perlindungan Informasi Keuangan di Sektor Publik

Assist. Prof. Dr. Ammar Ghazi Ibrahim Al-Ezzi, ammar.ezzi82@uodiyalaedu.iq (*)

Presidency of Diyala University, Baqubah, Diyala Governorate, Iraq

(*) Corresponding author

Abstract

General Background The rapid digital transformation in the public sector has increased reliance on electronic financial information systems, raising concerns about cybersecurity threats to financial data integrity. **Specific Background** Cyber risk governance has emerged as a strategic necessity, yet the organizational positioning of the accounting function within such frameworks remains unclear. **Knowledge Gap** Existing governance structures inadequately define the role of accounting in managing financially significant cyber risks, leading to institutional and structural misalignment. **Aims** This study aims to examine the integration of the accounting function into cyber risk governance and to propose an organizational framework that strengthens financial information protection. **Results** The findings reveal a significant organizational gap characterized by the absence of formal accounting roles, weak coordination between cybersecurity and financial policies, and limited involvement of accounting in risk assessment. **Novelty** The study introduces a multidimensional organizational framework that systematically integrates accounting into cyber risk governance through structural, functional, policy, and monitoring dimensions. **Implications** The proposed framework supports improved financial data security, enhanced transparency, and stronger accountability in public sector governance, contributing to more reliable financial reporting systems

Keywords: Cyber Risk Governance, Accounting Integration, Public Sector Governance, Financial Information Security, Organizational Framework

Key Findings Highlights

1. Structural exclusion of accounting roles limits coordination in digital risk management
2. Policy misalignment creates uncertainty in protecting governmental financial data
3. Multidimensional framework enables stronger institutional alignment and oversight

Published date: 2026-03-24

Vol. 21 No. 1 (2026): February
DOI: 10.21070/ijler.v21i1.1523

1. Introduction

Over the past few years, there has been an increasing rate of digital revolution in the public sector expressed in the number of electronic financial information systems that are used to conduct accounting operations and to prepare governmental reports. This has transformed the operations to make them more efficient, given them a quicker data processing time, and a higher level of financial transparency. Nonetheless, it has been coupled with growing cybersecurity threats to the integrity of financial information and the fidelity of governmental reporting.

The existence of cyber risks is now considered to be one of the most severe strategic and institutional risks that face public organizations. These risks could result in a data breach, financial information manipulation, or accounting system malfunction, thus, having a direct impact on the transparency, accountability, and good governance principles of the public sector. Therefore, the issue of cybersecurity risks cannot be treated as a purely technical challenge that is limited to the information technology department, but it has turned into a governance one which has its organizational and strategic aspects.

In this perspective, one of the key pillars of the internal control system and in protecting integrity of financial information is the accounting function. Accounting is the major provider of government financial reporting and hence any cyber threat on financial information has a direct impact on the quality and credibility of accounting information. Regardless of this essential connection, the role of accounting function in the cyber risk governance framework of most public institutions has not been defined appropriately. This state of affairs gets an organizational discontinuity between the need to govern cyber risk and the role of the accounting function.

To this end, the paper has sought to examine the incorporation of the accounting role in cyber risk governance and suggest a structure that would improve the protection of financial information in the government.

2. Research Problem

This has heightened the dependency on electronic financial information systems by the public institutions due to the continuous digital transformation of the institutions, thus putting financial information at a risk of cybersecurity attacks which can severely affect the integrity and reliability of financial information. Despite available general risk management frameworks, the organization placement of accounting function in cyber risk governance frameworks is not well defined. The lack of clarity poses an organizational disparity between the governance necessities of cybersecurity and the institutional mechanisms that are required to protect the financial information.

As such, this research problem can be formulated as follows:

What are some of the ways of integrating the accounting function into cyber risk governance frameworks in such a way that reinforces financial information security in the public sector?

3. Research Objectives

This study aims to:

1. Examine the principle of cyber risk management in the state sector and the connection between it and protection of financial information.

2. Indicate the organizational role and position of accounting function in cyberspace risk management framework.

3. Determine the organizational disparity between the cyber risk governance needs and the institutional role of accounting role in publicly-owned institutions.

4. Offer an organizational structure that will promote the empowering of the accounting role in cyber risk governance systems to improve the protection of financial information.

4. Research Questions

The following sub-questions are brought out by the main research question:

1. How is there a relationship between cyber risk governance and financial information protection in the public sector?

2. How evident is the accountability role of the accounting aspect in the cyber risk management practices?

3. How large is the organizational gap between the cyber risk governance requirements and the accounting role in the public institutions?

4. What can be done to structure an organizational setup that can strengthen the connection between the accounting role and the cyber risk governance systems?

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Vol. 21 No. 1 (2026): February
DOI: 10.21070/ijler.v21i1.1523

5. Research Importance

The relevance of this study is that it deals with a current situation that entails the merging of financial governance and the idea of cyber risk governance in the public sector, especially in the digital transformation era that has seen the overwhelming use of electronic financial information systems.

The following aspects explain the significance of the study:

1. Emphasizing the role of the accounting activity in the organization in safeguarding financial data against cybersecurity threats.

2. Making the knowledge gap concerning the integration of accounting into the cyber risk governance systems relevant.

3. Helping the decision-makers in the public sector by providing them with an organizational framework that helps in improving transparency and accountability.

4. Helping to develop the accounting thinking toward more integrative organizational positions in accordance with digital risk management.

6. Research Scope (Study Limitations)

The boundaries of this study are the following:

1. Thematic Scope: The research does not cover the topic of the accounting role in cyber risk governance beyond financial information protection, but rather solely in the technical context of more specific cybersecurity.

2. Institutional Scope: The discussion is limited to the government.

3. Temporal Scope: The research concerns the modern organizational context that is determined by the continuous digital transformation.

7. Research Methodology

The proposed research is characterized by a descriptive-analytical approach, which is suitable to look at the organizational phenomena and explain the correlations between the institutional roles and governance needs. The research approach to be used is the study of theoretical and regulatory provisions pertaining to cyber risk management and the inclusion of the accounting role in safeguarding financial data in the state sector. This is to determine the current organizational gap and create a recommended framework to be used to fill the gap.

The methodology of the research is as follows:

7.1 Theoretical Review

To find the conceptual basis of the study, a detailed overview of the literature and previous research on the issue of cyber risk governance, enterprise risk management, and the changing nature of the role of the accounting function in the digital environment.

7.2 Analysis of International Regulatory Frameworks

This will entail an analytical review of internationally accepted governance and risk management standards (which include the COSO, NIST and ISO 27001) that are broadly recognized as reference models of cyber risk and information governance [8],[3]. to identify organizational needs in terms of financial information protection and the level to which these frameworks acknowledge the accounting role in governance systems.

7.3 Organizational Gap Analysis

A conceptual comparative study of the requirements of cyber risk governance and real organizational positioning of the accounting role in the nonprofit sector to identify gaps and the level of institutional maladjustment.

7.4 Development of the Proposed Organizational Framework

The logical creation of a proposed organizational framework that explicitly presents the positioning and roles of the accounting function within cyber risk governance structures. The presented framework is based on the results of the theoretical study and identified organizational gap, and the goal is to improve the protection of financial information and strengthen the principles of good governance in the state sector.

The above theoretical foundation forms the analytical background of the paper to study cyber risk governance and diagnose the gap in the organization that is the focus of this research.

Indonesian Journal of Law and Economics Review
Vol. 21 No. 1 (2026): February
DOI: 10.21070/ijler.v21i1.1523

8. Theoretical Framework

8.1 Cyber Risk Governance in the Public Sector

The issue of cyber risks has become one of the major strategic threats to the general institutions, especially with the growing dependence on electronic financial information systems [12]. Cyber risk governance is the organizational structure, which outlines the policies, distributes responsibilities, and organizes the decision-makers to address digital threats that can destroy data integrity, especially governmental finances [8].

Cyber risk governance does not just entail the technical security of the systems; it includes strategic-level roles, organizational responsibility and endorsing transparency. In the government sector, the significance of the cyber risk governance is increased because it is directly connected to the protection of the public budget, the reputation of the financial reporting, and the trust of the citizens in the governmental institutions [6].

Cyber risk governance must be done through ensuring that roles are well assigned to sections of the organizational structure to facilitate coordination and integration between technical, financial, and administrative operations in safeguarding financial information against digital threats [5].

8.2 The Accounting Function within Cyber Risk Governance

Accounting activity is one of the essential foundations of the generation of government financial information, as well as its credibility [13]. The digital transformation has made its role not limited to the recording and disclosure activities as it is now closely connected to the integrity of the electronic financial processing systems and the quality of the generated data [12].

In this view, the accounting role can be considered as a part of an organization that can play its role in cyber risk governance by: [6], [1].

- Engaging in the process of identifying cyber risk to digital financial data .
- Understanding the possibility of cyber threats to affect financial reporting .
- Participating in the creation of financial data protection policies .
- Presentation of relevant information to senior management to help them make decisions on the risks that affect transparency and accountability.

Nonetheless, according to the experience in most governmental establishments, there are no well-spelled organizational roles given to the accounting role under cyber risk governance frameworks [12]. This ambiguity leaves a loophole in an organizational gap between the requirements of governance and the real institutional placement of the accounting function [8].

8.3 Organizational Gap Analysis

According to the organization literature, proper cyber risk governance involves transparency in assignments and the combination of technologic and financial processes to ensure the security of confidential information [5],[8]. But, in reality, practical experience shows that the management of cyber risks is usually the focus of technical departments, and the accounting department rarely participates in the evaluation of risks that have a significant impact on financial reporting [14].

The gap in the organization is manifested in a number of important dimensions which include: [2], [12], [20].

- The lack of a formally set organizational position of the accounting function to cyber risk governance committees.
- Minimal involvement of the accounting department in assessing the financial reporting of the cybersecurity breaches.
- The absence of policy coherency between financial disclosure policies and cybersecurity policies.
- The constriction of the role of the accounting function to the reactive fine-tuning of the events after they have occurred instead of the active participation in risk management.

This disconnect leads to poor financial and technical integration of both risk management perspectives, which leads to the low overall risk management effectiveness on cyber risk management in protecting financial information of government [5].

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Indonesian Journal of Law and Economics Review
Vol. 21 No. 1 (2026): February
DOI: 10.21070/ijler.v21i1.1523

Impact on Financial Information	Organizational Gap	Actual Accounting Practice	Cyber Risk Governance Requirements	Organizational Dimension
Weak financial–technical integration.	Absence of formal accounting positioning in cyber governance.	Cyber risk management concentrated in IT without accounting representation.	Formal inclusion of accounting within cyber governance structure.	Responsibility Structure
Risk to reporting accuracy and credibility.	Limited preventive accounting role in digital risk management.	Limited accounting involvement, mainly post-incident.	Proactive assessment of financially material cyber risks.	Financially Material Risk Assessment
Unclear financial protection mechanisms.	Lack of institutional integration between accounting and cyber governance.	Weak coordination between cybersecurity and financial policies.	Integration of cybersecurity and financial policies, including disclosure.	Policy Integration
Reduced effectiveness of financial risk governance.	Limited proactive participation in risk oversight.	Reactive accounting role focused on post-incident adjustments.	Continuous monitoring of financially relevant cyber risks.	Institutional Monitoring

Figure 1. Table 1. Organizational Gap Analysis between Cyber Risk Governance Requirements and the Institutional Positioning of the Accounting Function in the Public Sector

Source: Developed by the author based on the reviewed literature

8.3.1 Analysis of the Organizational Gap Findings

Table (1) concretizes the listed organizational gap by aligning the governance requirements with the current institutional practices. The comparison demonstrates structural exclusion of accounting function of cyber risk governance committees, it has limited functional involvement in financially material risk assessment and lacks policy integration between cybersecurity and financial governance functions. These results show that the gap is not only procedural, but structural and institutional, which compromises the systematic integration of financial oversight and the field of digital risk management in the public sector.

In addition, there is a poor integration between the policies of cybersecurity and financial governance policies, which leads to ambiguous institutional processes to protect financial information. This kind of misalignment can have an adverse impact on the quality and stability of financial reporting [2]. Thus, the lack of financial and technical integration of risk management decreases the overall risk management of cyber risk in safeguarding governmental financial information [5].

To fill this gap, therefore, involves the repositioning of the accounting role in the structure of cyber risk governance by means of designing a systematic approach that would facilitate the incorporation between the financial and technical aspects in the protection of governmental financial information.

9. Proposed Organizational Framework for Integrating the Accounting Function into Cyber Risk Governance

Due to the results of the organizational gap analysis, the current paper outlines an organizational framework that tries to reposition the role of the accounting aspect in cyber risk governance structures in the public sector [15]. The framework aims to guarantee that there is an integration between the financial and technical aspect in the protection of financial information in line with the current literature that underscores the need to have institutional integration in the management of digital risks [11].

The framework proposed is built on four organizational dimensions interrelated with each other:

Vol. 21 No. 1 (2026): February
DOI: 10.21070/ijler.v21i1.1523

9.1 Structural Dimension

The given framework formally uses the accounting function as part of the cyber risk governance framework by establishing its duties under organizational documents and internal policies accordingly with the information technology governance requirements in public institutions [18]. This dimension comprises: [9] ,[19].

1. Assuring formal coverage of the accounting role in the cyber risk governance committees.

2. The scope of its responsibility in relation to financially material cyber risks is clearly defined.

3. Incorporating the protection of financial information in its officially stipulated organizational responsibilities.

The aim of this dimension is to remove ambiguity in an organization concerning how the accounting role is placed in the digital risk management systems[16].

9.2 Functional Dimension

The suggested model focuses on the development of the functional area of the accounting position in order to incorporate [4], [20]. [7].

1. Being involved in defining cyber risks, which can undermine the integrity of financial information.

2. The effects of cybersecurity breaches or digital threats on financial reporting.

3. Investing funds in designing and developing cyber risk management policies.

With this growth the accounting role is now no longer reactive (post-incident) in nature, but rather proactive (risk assessment, governance) .

9.3 Policy Integration Dimension

The suggested framework denotes a need to attain systematic integration between [10], [17].

- Policies on information security.
- Financial governance policies.
- Disclosure and Transparency Requirements.

This merger is done by harmonizing the process of cybersecurity with the regulations of financial reporting, which will guarantee the institutional convergence and avoid the isolation of the technical and financial aspects. The rationale of this approach is evident in the studies on the significance of disclosure governance, financial reporting quality, and audit quality in the digital settings [1].

9.4 Institutional Monitoring Dimension

The framework suggested involves establishing institutional mechanisms that will be used in the sustained monitoring of the financial cyber risks.This includes: [7], [18].

- Acquiring cyber risk performance measurement into financial information administrative report.
- Determining the extent to which financial data has been exposed to online risks.
- Making periodic reports to the senior management about the risk that could befall the integrity and reliability of the financial reporting.

9.5 Expected Impact of the Proposed Framework

It is predicted that the proposed framework implementation will entail: [2] ,[9], [21]

- Enhance a combination of financial and technical aspects of risk management.
- Increase the security of governmental financial data.
- Strengthen the values of transparency and accountability.
- Minimise the chances of negative effects of cyber risks on credibility and reliability of financial reporting.

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Indonesian Journal of Law and Economics Review
Vol. 21 No. 1 (2026): February
DOI: 10.21070/ijler.v21i1.1523

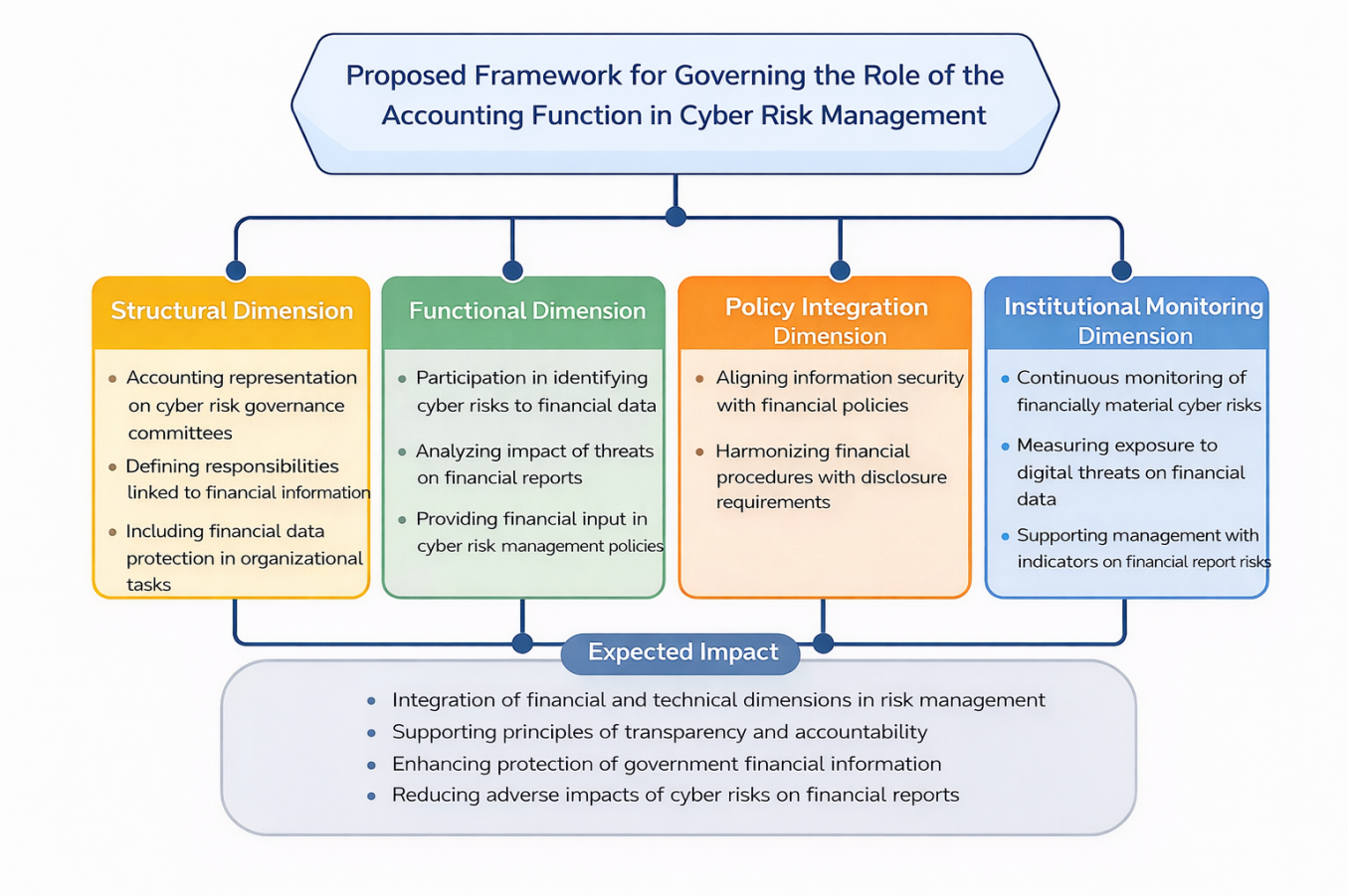

Figure 2. Figure (1): Proposed Organizational Framework for Integrating the Accounting Function into Cyber Risk Governance.

Source: Developed by the researcher based on the reviewed literature.

The figure demonstrates the offered organizational framework formed based on the recognized organizational gap between the requirements of the governance of cyber risks and the institutional role of the accounting function. It theorizes that structural integration, broadening of functional responsibility, integration of policies and sustained institutional surveillance are all constructive in terms of protection of financial information. The framework enhances the collaboration of financial and technical aspects and the improvement of transparency and accountability in the government sphere due to the systematic inoculation of the accounting role in the system of cyber risk governance.

10. Conclusions

According to the theoretical analysis, and the results of the organizational gap assessment, it is possible to make the following conclusions:

1. The public sector has become extremely vulnerable to cybersecurity threats with direct financial information implications due to digital transformation. The close connection between the processes of the digital transformation and the increase in cyber threats is verified by contemporary literature.

2. The research found an evident organizational discrepancy between the needs of cyber risk governance and the institutional role of the accounting role in the administrative system of the public sector.

3. Cyber risk management is still largely confined in technical departments with little or no accounting role in determining risks of financial materiality hence compromising on institutionalization in financial information security.

4. Lack of clearly defined roles of the accounting function as a part of the cyber risk governance frameworks lowers the effectiveness of governance and influences the negative outcome of transparency and accountability.

5. The suggested model of organization can help to redefine the institutional role of the accounting role in the system of

Vol. 21 No. 1 (2026): February
DOI: 10.21070/ijler.v21i1.1523

cyber risk governance and, therefore, contribute to improving the protection of financial information and ensuring the stability of government financial reporting.

11. Recommendations

Based on the results of the conducted study, the following recommendations can be made:

1. Incorporate the accounting functionality formally into cyber risk governance structures within the public institutions, and the responsibility of digital financial information is clearly defined among them.

2. Enlist accounting professionals actively in the process of detecting and gauging financially material cyber risks to enhance their active role in data protection.

3. Secure systematic convergence of the cybersecurity policies and financial governance policies in order to make information security procedures and disclosure requirements consistent with each other.

4. Establish institutional procedures to gauge the effects of cyber risks on the financial reporting and integrate the associated indicators in regular administrative reports.

5. Enhance. institutional sensitivity to the financial aspect of cyber risk management by using dedicated training and professional development opportunities on administrative and accounting staff.

References

1. M. H. A. Ahmed, “Disclosure of Cybersecurity Risk Management Strategies Within Cybersecurity Risk Reports: Motivations, Challenges and Development Mechanisms,” Accounting Innovation Journal, vol. 2, no. 1, 2025.
2. M. A. S. Al-Krewi, “Measuring the Impact of Cybersecurity Risks on the Financial Resilience of Banking Institutions in a Digital Transformation Environment: A Field Study on Jumhouria Bank – Misrata Branch,” Libyan Journal of Contemporary Academic Studies, vol. 4, no. 1, pp. 107–128, 2026.
3. I. M. Al-Qasir, “Information Technology Governance to Reduce Cyber Risks and Enhance the Security of Accounting Information in Libyan Public Institutions: A Proposed Model,” Journal of Academic Research (Administrative & Financial Sciences), vol. 28, no. 2, 2024.
4. S. A. M. Badran, “The Impact of Cybersecurity Governance on Audit Quality,” Journal of Financial and Commercial Research, vol. 26, no. 4, 2025.
5. F. H. O. Kolo et al., “Mitigating Cybersecurity Risks in Financial Institutions Through Strategic Third-Party Risk Governance Frameworks,” Journal of Engineering Research and Reports, vol. 27, no. 5, pp. 173–193, 2025, doi:10.9734/jerr/2025/v27i51501.
6. K. I. Milad and F. M. Abu Shafaa, “The Role of Accounting Disclosure on Cybersecurity in Improving the Quality of Accounting Information in Libyan Commercial Banks: An Applied Study,” Human and Natural Sciences Journal, vol. 6, no. 7, 2025, doi:10.53796/hnsj67/37.
7. S. O. Olawore et al., “AI-Driven Cybersecurity Governance in Financial Services: Ethical Auditing, Automated Compliance Monitoring and Explainable AI for Stakeholder Trust,” IRE Journals, vol. 8, no. 10, 2025.
8. L. Qudus, “Cybersecurity Governance: Strengthening Policy Frameworks to Address Global Cybercrime and Data Privacy Challenges,” International Journal of Science and Research Archive, vol. 14, no. 1, pp. 1146–1163, 2025, doi:10.30574/ijsra.2025.14.1.0225.
9. A. S. A. Riyadh, “Data Protection and Privacy in the Digital Environment: A Comparative Study Between the University of California, Berkeley and Ain Shams University,” Fayoum University Journal of Educational & Psychological Sciences, vol. 19, no. 17, 2025.
10. U. F. Saeed and A.-K. Mohammed, “Do Debt Financing, Tech-Driven Transformation and Corporate Governance Constrain Financial Reporting Quality? Evidence from China,” Cogent Economics & Finance, vol. 13, no. 1, 2025, doi:10.1080/23322039.2025.2521467.
11. A. A. A. Shannan, “A Proposed Accounting Model for the Relationship Between Cybersecurity Risk Disclosure Governance and Cost of Financing in Light of Contemporary Professional Releases: An Applied Study on Egyptian Listed Companies,” Scientific Journal of Financial and Commercial Studies, vol. 7, no. 1, pp. 929–949, 2026.
12. V. Shepeliuk, “Digital Transformation of Accounting and Analytical Processes in Ukraine: Trends, Challenges, and Security Imperatives (2020–2025),” Economics, Finance and Management Review, no. 3, pp. 58–66, 2025, doi:10.36690/2674-5208-2025-3-58-66.
13. M. Sekinobe et al., “An Interdisciplinary Framework for the Development of Intelligent Accounting Automation Systems Integrating Predictive Risk Analytics and Dynamic Internal Control Mechanisms,” International Journal of Innovative Science and Research Technology, vol. 10, no. 12, pp. 2520–2533, 2025, doi:10.38124/ijisrt/25dec1138.
14. O. O. Ajakaye et al., “Integrating Artificial Intelligence in Organizational Cybersecurity: Consumer Data Protection in the U.S. Fintech Sector,” World Journal of Advanced Research and Reviews, vol. 26, no. 1, pp. 2802–2821, 2025, doi:10.30574/wjarr.2025.26.1.1421.
15. I. F. Awolowo et al., “Cybersecurity Assurance for SMEs: A Conceptual Framework Integrating Organizational Culture, Fraud Risk Management and Forensic Accounting,” Canadian Journal of Administrative Sciences, vol. 43, 2026, doi:10.1002/cjas.70051.
16. A. Dash, “Blockchain and AI in Corporate Governance: New Frontiers for Accounting Education in India’s Financial Sector,” Grazing Minds Journal of Management Innovation and Technology, 2024.

Vol. 21 No. 1 (2026): February
DOI: 10.21070/ijler.v21i1.1523

17. Y. Biliavska et al., “Monitoring of Cyber Risks in the Financial Sector of the Economy,” Financial and Credit Activity: Problems of Theory and Practice, vol. 3, no. 62, 2025, doi:10.55643/fcaptp.3.62.2025.4702.
18. O. Chumak et al., “Information Protection and Cyber Security in the Public and Financial Sectors,” Edelweiss Applied Science and Technology, vol. 8, no. 5, pp. 1164–1174, 2024, doi:10.55214/25768484.v8i5.1819.
19. O. Akimova et al., “Cyber Protection of Financial Data in Accounting: Implementation and Use of Cryptographic Techniques,” Economic Affairs, vol. 69, no. 2, pp. 1041–1052, 2024, doi:10.46852/0424-2513.3.2024.27.
20. J. H. Senanu, “Insider Threats and Privilege Misuse in Financial Service Delivery: A Cyber-Resilience and Financial Sector Risk Framework,” 2024.
21. L. Hasan et al., “Cybersecurity in Accounting: Protecting Financial Data in the Digital Age,” European Journal of Applied Science, Engineering and Technology, vol. 2, no. 6, pp. 64–80, 2024, doi:10.59324/ejaset.2024.2(6).06.

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo