Acta Universitatis Danubius
ŒCONOMICA

Integrating the Accounting Function into Cyber Risk Governance: A Proposed Organizational Framework to Strengthen Financial Information Protection in the Public Sector

Ammar Ghazi Ibrahim Al-Ezzi[1]

Abstract: Objectives: This paper aims to discuss the integration of the accounting function into cyber risk governance in order to strengthen the protection of financial information in the public sector within the context of digital transformation. **Prior Work:** Previous studies on cyber risk governance have primarily focused on technical and regulatory dimensions, while limited attention has been given to the organizational role of the accounting function in addressing financially material cyber risks and protecting financial information. **Approach:** The study adopts a descriptive–analytical approach based on the review of relevant literature, governance frameworks, and prior studies. It also analyses the organizational gap between cyber risk governance requirements and the actual practices of public sector institutions. **Results:** The findings reveal a significant organizational gap reflected in the limited formal involvement of the accounting function in cyber risk management processes, as well as weak alignment between cybersecurity policies and financial governance mechanisms. **Implications:** The study highlights the importance of strengthening the institutional role of the accounting function within cyber risk governance frameworks to improve financial information protection, accountability, transparency, and institutional resilience in the public sector. **Value**: This paper provides an organizational perspective by proposing a framework that integrates the accounting function into cyber risk governance, thereby addressing an important gap that has received limited attention in previous literature.

Keywords: Cybersecurity Risk; Financial Reporting; Risk Assessment; Government Sector; Internal Control.

[1] Assist. Prof. Dr., Department of Accounting, College of Administration and Economics, University of Diyala, Baqubah, Diyala Governorate, Iraq, Corresponding author: ammar.ezzi82@uodiyala.edu.iq.

JEL Classification: M41; G32; H83

1. Introduction

The last several years have been characterized by a breakneck pace of digitalization of the public sector, especially the proliferation of electronic financial information systems to help with accounting operations and governmental reporting. Nevertheless, it has also been threatened by the growth it has of cybersecurity threats which can impact the integrity of financial data and credibility of governmental reports.

Cyber risks have become one of the most significant strategic and institutional challenges of public organizations. Such risks can cause data breach, financial information manipulation or interference with the accounting systems that directly impact transparency, accountability and good governance practices. Cybersecurity is thus no longer a technical problem, that is, confined to IT departments, but a problem of governance, with definite organizational and strategic aspects.

The accounting function in this context is one of the major parts of the internal control system and is critical in safeguarding the integrity of financial information. Although this is a significant relationship, it is not well understood that accounting function can play in cyber risk governance systems in most public institutions. This scenario creates an organizational gap between governance needs and the institutional role of accounting.

To that end, the paper will discuss the way in which the accounting role can be incorporated into the cyber risk governance and suggest an organizational structure to enhance the security of financial information in the public sector.

2. Research Problem

The ongoing digital revolution within the state institutions has made them more reliant on electronic financial information systems. This has exposed financial data to cybersecurity threats that can impact its integrity and reliability. Although there are general risk management frameworks, the accounting function within cyber risk governance frameworks has not been well placed in an organization. Such ambiguity establishes an organizational gap between the requirements of cybersecurity

governance and the institutional mechanisms that are required to secure financial information.

In this connection, it is possible to state the following research problem:

What role can the accounting function play in cyber risk governance systems to enhance the security of financial information in the public sector?

3. Research Objectives

This study aims to:

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

• Indicate the organizational role and position of accounting function in cyberspace risk management framework;

• Determine the organizational disparity between the cyber risk governance needs and the institutional role of accounting role in publicly owned institutions;

• 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:

• What is the relationship between cyber risk governance and financial information protection in the public sector?

• What is the role of the accounting function in cyber risk management practices?

• What is the extent of the organizational gap between cyber risk governance requirements and the accounting role in public institutions?

• How can an organizational structure be developed to strengthen the link between the accounting function and cyber risk governance systems?

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:

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

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

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

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

• Research Scope (Limitations in the study)

This research paper has the following scope:

• Thematic Scope: The article is about the importance of accounting function in the reduction of cyber risks through financial information security.

• Institutional Scope: The topic of the study is restricted to institutions of a public sector.

• Temporal Scope: The work deals with the present situation in the organization under digital transformation.

6. 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:

6.1. 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.

6.2. Analysis of International Regulatory Frameworks

This will entail an analytical review of internationally accepted governance and risk management standards (which include the COSO, NIST & ISO 27001) that are broadly recognized as reference models of cyber risk and information governance (Qudus, 2025; Al-Qasir, 2024) to identify organizational needs in terms of financial information protection and the level to which these frameworks acknowledge the accounting role in governance systems.

6.3. 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.

6.4. 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 theoretical study and identified organizational gaps, 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.

7. Theoretical Framework

7.1. 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 (Shepeliuk, 2025). 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 (Qudus, 2025).

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 (Milad & Abu Shafaa, 2025).

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 (Kolo et al., 2025).

7.2. 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. 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 (Shepeliuk, 2025).

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: (Milad & Abu Shafaa, 2025; Ahmed, 2025).

• 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 (Shepeliuk, 2025). This ambiguity leaves a loophole in an organizational gap between the requirements of governance and the real institutional placement of the accounting function (Qudus, 2025).

7.3. 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(Qudus, 2025; Kolo et al., 2025), 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 (Milad & Abu Shafaa, 2025, Kolo et al., 2025).

The gap in the organization is manifested in a number of important dimensions which include: (Al-Krewi, 2026; Shepeliuk, 2025; Senanu, 2024).

• 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.

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

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*

Source: Developed by the author based on the reviewed literature

7.3.1. 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.

This kind of misalignment can have an adverse impact on the quality and stability of financial reporting (Al-Krewi, 2026). Thus, the lack of financial and technical integration of risk management decreases the overall risk management of cyber risk in safeguarding governmental financial information (Kolo et al., 2025).

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.

8. 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 (Awolowo et al.,2026). The framework aims to guarantee that there is an integration between the financial and technical aspects 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 (Qudus, 2025).

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

8.1. 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 according to the information technology governance requirements in public institutions (Al-Qasir, 2024). This dimension comprises: (Akimova et al., 2024; Riyadh, 2025).

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

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

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

8.2. Functional Dimension

The suggested model focuses on the development of the functional area of the accounting position in order to incorporate: (Olawore et al., 2025; Badran, 2025; Shannan, 2026).

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

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

• 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), (Al-Krewi, 2026).

8.3. Policy Integration Dimension

The suggested framework denotes a need to attain systematic integration between (Saeed & Mohammed, 2025; Ahmed, 2025; Badran, 2025).

• Policies on information security.

• Financial governance, disclosure, and transparency requirements.

This merger is done by harmonizing the process of cybersecurity with the regulations of financial reporting, which will guarantee 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.

8.4. Institutional Monitor

ing Dimension

The framework suggested involves establishing institutional mechanisms that will be used in the sustained monitoring of the financial cyber risks.This includes: (Chumak et al,2024; Olawore et al, 2025).

• 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.

8.5. Expected Impact of the Proposed Framework

It is predicted that the proposed framework implementation will entail: (Hasan et al., 2024; Riyadh, 2025; Al-Krewi, 2026).

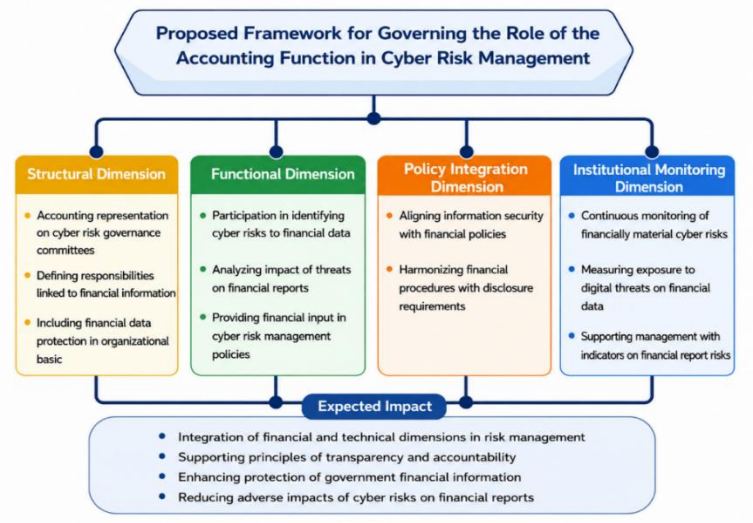
• Enhance a combination of financial and technical aspects of risk management.

• 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.

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 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.

9. Conclusions

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

• 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 digital transformation and the increase in cyber threats is verified by contemporary literature.

• 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.

• 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.

• 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.

• The suggested model of organization can help to redefine the institutional role of the accounting role in the system of cyber risk governance and, therefore, contribute to improving the protection of financial information and ensuring the stability of government financial reporting.

10. Recommendations

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

• 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.

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

• 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.

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

• 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

Ahmed, M. H. A. (2025). Disclosure of cybersecurity risk management strategies within cybersecurity risk reports: Motivations, challenges and development mechanisms. *Accounting Innovation Journal, 2*(1).

Ajakaye, O. O., Olanrewaju, A. G., Fawehinmi, D., Afolabi, R., & Pius-Kiate, G. M. (2025). Integrating artificial intelligence in organizational cybersecurity: Enhancing consumer data protection in the U.S. fintech sector. *World Journal of Advanced Research and Reviews, 26*(1), 2802–2821. https://doi.org/10.30574/wjarr.2025.26.1.1421

Akimova, O., Oliinyk, O., Holovko, O., Kreviazuk, I., & Yashchenko, Y. (2024). Cyber protection of financial data in accounting: Implementation and use of cryptographic techniques. *Economic Affairs, 69*(2), 1041–1052. https://doi.org/10.46852/0424-2513.3.2024.27

Al-Krewi, M. A. S. (2026). 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, 4*(1), 107–128.

Al-Qasir, I. M. (2024). 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), 28*(2).

Awolowo, I. F., Garuba, A. O., Nwankwo, C. E., & Adeyemo, K. A. (2026). Cybersecurity assurance for SMEs: A conceptual framework integrating organizational culture, fraud risk management and forensic accounting. *Canadian Journal of Administrative Sciences, 43*. https://doi.org/10.1002/cjas.70051

Badran, S. A. M. (2025). The impact of cybersecurity governance on audit quality. *Journal of Financial and Commercial Research, 26*(4).

Biliavska, Y., Kucherova, H., Rudenko, M., Nazarenko, I., & Dzhyndzhoian, V. (2025). Monitoring of cyber risks in the financial sector of the economy. *Financial and Credit Activity: Problems of Theory and Practice, 3*(62). https://doi.org/10.55643/fcaptp.3.62.2025.4702

Chumak, O., Koval, V., Hrytsenko, O., Datsiuk, O., & Kovalenko, V. (2024). Information protection and cyber security in the public and financial sectors. *Edelweiss Applied Science and Technology, 8*(5), 1164–1174. https://doi.org/10.55214/25768484.v8i5.1819

Dash, A. (2024). Blockchain and AI in corporate governance: New frontiers for accounting education in India's financial sector. *Grazing Minds Journal of Management Innovation and Technology.*

Hasan, L., Rahman, M. A., Karim, S., & Hossain, M. T. (2024). Cybersecurity in accounting: Protecting financial data in the digital age. *European Journal of Applied Science, Engineering and Technology, 2*(6), 64–80. https://doi.org/10.59324/ejaset.2024.2(6).06

Kolo, F. H. O., Adekunle, A. A., Ibrahim, M. S., & Yusuf, R. M. (2025). Mitigating cybersecurity risks in financial institutions through strategic third-party risk governance frameworks. *Journal of Engineering Research and Reports, 27*(5), 173–193. https://doi.org/10.9734/jerr/2025/v27i51501

Milad, K. I., & Abu Shafaa, F. M. (2025). 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, 6*(7). https://doi.org/10.53796/hnsj67/37

Olawore, S. O., Adeyemi, T. A., Okonkwo, C. J., & Ibrahim, A. M. (2025). AI-driven cybersecurity governance in financial services: Enhancing ethical auditing, automated compliance monitoring and explainable AI for stakeholder trust. *IRE Journals, 8*(10).

Qudus, L. (2025). Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges. *International Journal of Science and Research Archive, 14*(1), 1146–1163. https://doi.org/10.30574/ijsra.2025.14.1.0225

Riyadh, A. S. A. (2025). 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, 19*(17).

Saeed, U. F., & Mohammed, A.-K. (2025). Do debt financing, tech-driven transformation and corporate governance enhance or constrain financial reporting quality? Evidence from China. *Cogent Economics & Finance, 13*(1). https://doi.org/10.1080/23322039.2025.2521467

Sekinobe, M., Nansubuga, R., Kato, J., & Mugisha, P. (2025). 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, 10*(12), 2520–2533. https://doi.org/10.38124/ijisrt/25dec1138

Senanu, J. H. (2024). Insider threats and privilege misuse in financial service delivery: A cyber-resilience and financial sector risk framework.

Shannan, A. A. A. (2026). 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, 7*(1), 929–949.

Shepeliuk, V. (2025). Digital transformation of accounting and analytical processes in Ukraine: Trends, challenges, and security imperatives (2020–2025). *Economics, Finance and Management Review*, (3), 58–66. https://doi.org/10.36690/2674-5208-2025-3-58-66