The Role of Audit Committee in Cyber Risk Governance and Accountability: A Literature Review Perspective

Okor Eno Eyo
Department of Accountancy
University of Cross River State, Calabar
https://doi.org/10.56201/jafm.vol.12.no9.2026.p10.17

Abstract
The study examined the role of audit committee in cyber risk governance and accountability. *The audit committee can contribute by reviewing cyber risk assessments, monitoring the effectiveness of internal controls, questioning management on cybersecurity preparedness and ensuring that significant cyber risks are appropriately communicated to the board and relevant stakeholders. Cyber risk governance is particularly important because weak oversight can create gaps between an organisation's cybersecurity policies and their actual implementation. The study recommended that organisations should strengthen the independence of audit committee members by ensuring that the committee is composed predominantly of members who can exercise objective judgement without undue influence from management. Also, organisations should ensure that audit committees possess adequate cybersecurity, information technology, accounting, auditing and risk-management expertise.*

Keywords: *Audit committee, cyber risk governance, accountability, cyber risk assessments, internal controls,*

Introduction

The rapid adoption of digital technologies has transformed the way organisations conduct business, manage information and deliver services, but it has also increased exposure to cyber threats such as data breaches, ransomware, identity theft and unauthorised access. Cybersecurity has therefore moved beyond a purely technical concern to become a major corporate governance and accountability issue. Effective cyber risk governance requires organisations to establish appropriate oversight structures that identify cyber risks, strengthen internal controls and ensure that management remains accountable for protecting critical information assets (Kshetri, 2021; World Economic Forum, 2024). Within this governance structure, the audit committee plays an increasingly important role in providing independent oversight of risk management, internal control and financial reporting processes. Although cybersecurity may traditionally have been regarded as the responsibility of information technology departments, the potential financial, regulatory and reputational consequences of cyber incidents make it a matter requiring board and audit committee attention. The audit committee can contribute by reviewing cyber risk assessments, monitoring the effectiveness of internal controls, questioning management on cybersecurity preparedness and ensuring that significant cyber risks are appropriately communicated to the board and relevant stakeholders (Institute of Internal Auditors, 2023; National Institute of Standards and Technology, 2024).

Cyber risk governance is particularly important because weak oversight can create gaps between an organisation's cybersecurity policies and their actual implementation. An effective audit committee can enhance accountability by demanding reliable risk information, evaluating management responses to identified vulnerabilities and ensuring that corrective actions are implemented. This oversight function can also strengthen organisational transparency and confidence among shareholders, regulators, customers and other stakeholders. Consequently, examining the role of the audit committee in cyber risk governance and accountability is essential for understanding how corporate governance mechanisms can contribute to organisational resilience and responsible management of digital risks.

Theoretical Framework

The theoretical framework provides the intellectual foundation for examining the relationship between audit committee characteristics and cyber risk governance and accountability. The increasing dependence of organisations on digital technologies has made cyber risk an important corporate governance concern. Consequently, the responsibility for managing cyber risks is no longer restricted to information technology personnel but extends to boards of directors, audit committees, internal auditors and other governance actors. This study is anchored on Agency Theory and supported by Resource Dependence Theory. Agency Theory provides the principal theoretical foundation because it explains the monitoring and accountability responsibilities of the audit committee, while Resource Dependence Theory explains the importance of knowledge, expertise and other resources provided by audit committee members in addressing complex cyber risks.

Agency Theory

Agency Theory was formally developed by Jensen and Meckling (1976) to explain the relationship between principals and agents within organisations. The theory argues that shareholders or owners (principals) delegate decision-making authority to managers (agents) to manage organisational resources on their behalf. However, the interests of managers may not always correspond with those of shareholders. This divergence of interests creates agency problems, particularly where managers possess more information about organisational activities than shareholders. The resulting information asymmetry creates the need for effective monitoring and control mechanisms to ensure that managers act in the best interests of the organisation. The audit committee represents one of the important governance mechanisms for reducing agency problems. Its responsibility for reviewing financial reporting, internal controls, risk management and internal audit activities provides an additional layer of monitoring over management. In the context of cyber risk, the relevance of Agency Theory is even more pronounced because cybersecurity information is often highly technical and asymmetrical. Management and information technology personnel may possess significantly more knowledge about an organisation's cyber vulnerabilities, security controls and incident exposures than board members and shareholders. This information asymmetry can make it difficult for principals to determine whether management is adequately addressing cyber risks. An effective audit committee can reduce this information gap by demanding reliable cybersecurity information, reviewing internal controls and challenging management's assessment of cyber threats. Audit committee independence is particularly important because independent members are more capable of exercising objective judgement and challenging management without undue influence. Similarly, audit committee expertise enables members to understand accounting, risk-management, information technology and cybersecurity

issues and to evaluate management's responses appropriately. Audit committee diligence is also consistent with Agency Theory because regular meetings, review of risk reports and follow-up on identified control weaknesses increase the intensity of managerial monitoring. In addition, an appropriately constituted audit committee size can provide adequate monitoring capacity and allow members to bring diverse perspectives to the assessment of organisational risks. Through these mechanisms, the audit committee can reduce information asymmetry, strengthen internal controls and improve management accountability.

Literature Review

Audit Committee Independence

Audit committee independence refers to the degree to which members of the audit committee are free from relationships or interests that could compromise their objectivity in monitoring management. Independence is important because effective cyber risk governance requires committee members to challenge management's cybersecurity decisions rather than merely endorse them. An independent audit committee is more likely to demand adequate information about cyber threats, question weaknesses in internal controls and insist that identified vulnerabilities are addressed. The importance of independent oversight has become more pronounced as cybersecurity has developed into an enterprise-level risk. Contemporary governance guidance recognizes that cyber risk can affect organisational operations, financial performance, regulatory compliance and reputation. NIST (2024) therefore places governance at the center of cybersecurity risk management, emphasizing the need for organizational leadership to establish, communicate and monitor cybersecurity expectations. From an accountability perspective, audit committee independence can strengthen the monitoring relationship between the board and management. Independent members can require management to provide transparent reports on cyber incidents, cybersecurity investments, risk exposures and remedial actions. This reduces the possibility of management withholding unfavorable cybersecurity information. Deloitte also identifies proactive audit committee engagement as an important component of cyber risk oversight where the responsibility has been delegated to the committee. Therefore, a higher degree of audit committee independence is expected to enhance effective cyber risk governance and organizational accountability.

Audit Committee Expertise

Audit committee expertise refers to the knowledge and professional competence possessed by committee members in areas relevant to their oversight responsibilities. While traditional audit committee expertise has focused largely on accounting, auditing and financial reporting, the increasing complexity of digital risks makes technological and cybersecurity knowledge increasingly valuable. Cybersecurity decisions often involve highly technical issues relating to data protection, information systems, cloud computing, cyber threats, incident response and digital controls. Committee members without adequate knowledge may find it difficult to understand management's cybersecurity reports or challenge technical assumptions. Dziwa (2023) argues that effective board and audit committee oversight requires members with knowledge spanning finance, accounting, technology and cybersecurity. The relevance of expertise is further demonstrated by current corporate governance practice. Research and governance surveys increasingly identify cybersecurity expertise as an important consideration at board and committee level. Audit committees are also increasingly involved in cybersecurity oversight, rather than limiting their responsibilities to financial reporting and traditional internal controls. An audit committee with

appropriate cybersecurity and technology expertise is consequently better positioned to assess cyber risk reports, evaluate internal controls, understand emerging threats and hold management accountable for cybersecurity performance. Thus, audit committee expertise is expected to have a positive effect on cyber risk governance and accountability.

Audit Committee Diligence and Cyber Risk Governance and Accountability

Audit committee diligence refers to the extent to which the committee actively performs its oversight responsibilities through regular meetings, careful review of reports, engagement with management and auditors, and follow-up on identified risks. Diligence is particularly important in cybersecurity because cyber threats evolve rapidly and cannot be effectively managed through occasional or reactive oversight. A diligent audit committee should regularly review the organization's cybersecurity risk profile, significant incidents, internal control weaknesses, regulatory requirements and management's response to identified threats. The committee should also ensure that unresolved cybersecurity issues are followed through until corrective actions are implemented. The increasing importance attached to cybersecurity in audit committee agendas supports this argument. Recent evidence indicates that cybersecurity has become one of the leading priorities for audit committees, with many committees assigning significant attention to cyber risk alongside enterprise risk management, compliance and internal audit.

Lanz (2023) similarly observes that audit committee cybersecurity oversight has expanded beyond simply responding to breaches to include regulatory compliance, stakeholder expectations and a deeper understanding of the risks associated with an organization's digital activities. Consequently, an audit committee that meets regularly, reviews cybersecurity information carefully and follows up on identified weaknesses is more likely to promote effective cyber risk governance and stronger organizational accountability.

Audit Committee Size

Audit committee size refers to the number of members serving on the audit committee. Committee size can influence the availability of knowledge, experience, perspectives and monitoring capacity. A committee with an adequate number of members may be better positioned to distribute responsibilities, evaluate complex cybersecurity information and provide effective oversight. Cyber risk governance requires consideration of several interconnected issues, including internal controls, financial implications, data protection, regulatory compliance, information technology and business continuity. A committee with sufficient membership may therefore provide a broader range of expertise and perspectives when evaluating these issues. However, larger committee size does not automatically guarantee effectiveness. Excessive membership may create coordination difficulties, reduce individual accountability and make decision-making less efficient. The important issue is therefore whether the committee is sufficiently sized to provide effective oversight while maintaining active participation by individual members.

Current governance practice shows that audit committees are increasingly being given responsibility for cybersecurity oversight. For example, Deloitte reports that audit committees are frequently assigned primary responsibility for cyber risk oversight, although responsibility may also rest with the full board or another specialised committee. An appropriately constituted audit committee can therefore provide the capacity needed to review cyber risks, challenge management and monitor accountability. The study consequently expects audit committee size to influence cyber risk governance and accountability.

Empirical Literature

Empirical studies have increasingly examined the relationship between corporate governance mechanisms and cybersecurity risk management, particularly as cyber threats have become an important concern for organisations and their stakeholders. One of the important governance mechanisms receiving attention is the audit committee because of its responsibility for monitoring internal controls, risk management and management accountability. Existing studies have examined different characteristics of audit committees, including independence, expertise, diligence and size, although the findings and areas of emphasis differ across studies. Ojeka, Ben-Caleb, and Ekpe (2017) examined cybersecurity in the Nigerian banking sector with particular emphasis on audit committee effectiveness. Using a sample of 13 listed Nigerian banks, the study investigated audit committee independence, financial expertise and technological expertise in relation to cybersecurity compliance. The researchers employed correlation and ordinary least squares regression techniques and found that audit committee independence, financial expertise and technological expertise did not have significant positive relationships with cybersecurity compliance. The study concluded that the composition and expertise of audit committees in Nigerian banks were not sufficiently developed to provide effective cybersecurity oversight. The authors consequently recommended greater inclusion of technological and financial experts as well as genuinely independent members on audit committees. Although the study provides important evidence from Nigeria, its findings also reveal the need for further investigation, particularly because the cybersecurity environment has changed considerably since the study was conducted.

Building on the importance of technological expertise identified in earlier research, Smith et al. (2021) investigated cybersecurity breaches and the role of information technology governance in audit committee charters. Using a sample of 189 firms, the study examined whether cybersecurity incidents and the existence of technology committees influenced the extent to which information technology governance responsibilities were assigned to audit committees. The findings indicated that organisations experiencing cybersecurity breaches were more likely to explicitly assign IT governance responsibilities to their audit committees. The study therefore demonstrated that cyber incidents can influence the governance structure and responsibilities of audit committees. This finding extends the argument of Ojeka et al. (2017) by showing that audit committees are increasingly being recognised as relevant governance mechanisms for addressing technological and cybersecurity risks. However, the study focused largely on the formal assignment of IT governance responsibilities rather than examining how specific audit committee characteristics influence actual cyber risk governance and accountability.

The importance of expertise was further demonstrated by Bhattacharjee et al. (2024), who investigated board oversight of cybersecurity using field evidence. Their study examined the ability of directors to provide meaningful cybersecurity oversight and found that non-expert directors could engage in cybersecurity oversight, but their efforts were sometimes symbolic because of inadequate technical knowledge. Directors with relevant expertise were better positioned to identify weaknesses and encourage stronger cybersecurity capabilities within organisations. The study consequently established that effective cybersecurity oversight requires not only the existence of governance structures but also the knowledge necessary to understand complex cyber risks. This finding is particularly relevant to audit committee expertise because members who possess information technology and cybersecurity knowledge are more likely to understand cyber risk reports and critically assess management's responses. Nevertheless, the study focused primarily on board-level expertise, leaving an opportunity to examine the specific contribution of audit committee expertise alongside other audit committee characteristics.

More recent evidence was provided by Guohong, Zhongwei, Feng, and Zhongyi (2025), who examined the effect of audit committee IT expertise on corporate cybersecurity risk disclosure among Chinese listed firms. The study found that firms whose audit committees possessed greater IT expertise provided more extensive and higher-quality cybersecurity risk disclosures. The relationship was particularly evident in firms experiencing greater information asymmetry and weaker governance conditions. The study further suggested that improvements in internal control and information disclosure quality provide possible channels through which audit committee IT expertise enhances cybersecurity risk disclosure. These findings strengthen the position of Bhattacharjee et al. (2024) by demonstrating empirically that technological expertise within the audit committee can translate into improved cybersecurity-related corporate reporting. However, the study concentrated on cybersecurity risk disclosure rather than the broader concept of cyber risk governance and accountability adopted in the present study.

Similarly, Gao and Calderon (2025) examined cybersecurity risk governance and cybersecurity risk disclosures in corporate 10-K filings. Their study considered the increasing involvement of boards and board-level committees in cybersecurity oversight and investigated whether governance arrangements and cybersecurity expertise were associated with the quality of cyber-risk disclosure. The findings indicated that stronger cybersecurity governance and relevant expertise were associated with more detailed and specific cybersecurity risk disclosures. The study also showed that audit committees were among the most common governance bodies assigned responsibility for cybersecurity oversight. This finding reinforces the evidence from Guohong et al. (2025) that governance structures and technological expertise are important for effective cybersecurity oversight. However, the study primarily concentrated on cybersecurity disclosure and governance arrangements and did not comprehensively examine audit committee independence, diligence and size as separate determinants.

Taken together, the empirical studies demonstrate a developing relationship between audit committee characteristics and cybersecurity governance. Ojeka et al. (2017) provided Nigerian evidence on audit committee independence and expertise, while Smith et al. (2021) demonstrated that cybersecurity incidents can increase the formal cybersecurity responsibilities assigned to audit committees. Bhattacharjee et al. (2024) subsequently established the importance of cybersecurity expertise for meaningful oversight, while Guohong et al. (2025) and Gao and Calderon (2025) provided more recent evidence that audit committee and board-level cybersecurity expertise and governance arrangements can improve cybersecurity risk disclosure and oversight. Although these studies provide valuable evidence, there remains limited empirical attention to the combined influence of audit committee independence, expertise, diligence and size on cyber risk governance and accountability, particularly within the Nigerian context. The present study therefore seeks to extend existing literature by examining these four audit committee dimensions simultaneously and determining their influence on cyber risk governance and accountability.

Conclusion and Recommendations

Cyber risk governance is particularly important because weak oversight can create gaps between an organisation's cybersecurity policies and their actual implementation. An effective audit committee can enhance accountability by demanding reliable risk information, evaluating management responses to identified vulnerabilities and ensuring that corrective actions are implemented. The following recommendations are proffered thus:

1. Organisations should strengthen the independence of audit committee members by ensuring that the committee is composed predominantly of members who can exercise objective judgement without undue influence from management.
2. Organisations should ensure that audit committees possess adequate cybersecurity, information technology, accounting, auditing and risk-management expertise.
3. The committee should periodically review cybersecurity reports, risk assessments, incident-response plans, internal-control weaknesses and management's progress in implementing corrective measures.

References

Bhattacharjee, S., et al. (2024). *Inexpert supervision: Field evidence on boards' oversight of cybersecurity*. Management Science.

Dziwa, A. A. (2023). *Governance and board oversight do matter*. ISACA Now.

Gao, L., & Calderon, T. G. (2025). Cybersecurity risk governance and companies' cybersecurity risk disclosures in their 10-K filings. *Journal of Accounting and Public Policy*, 54, 107376.

Guohong, Z., Zhongwei, X., Feng, H., & Zhongyi, X. (2025). The audit committee's IT expertise and its impact on the disclosure of cybersecurity risk. *Research in International Business and Finance*, 73, 102542. https://doi.org/10.1016/j.ribaf.2024.102542

Institute of Internal Auditors. (2020). *Assessing cybersecurity risk: The three lines model*. The Institute of Internal Auditors.

Institute of Internal Auditors. (2024). *Auditing cyber incident response and recovery*. The Institute of Internal Auditors.

Institute of Internal Auditors. (2025). *Auditing cybersecurity operations: Prevention and detection* (2nd ed.). The Institute of Internal Auditors.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behaviour, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305–360.

Lanz, J. (2023). The audit committee's oversight for cybersecurity. The CPA Journal.

Ojeka, S. A., Ben-Caleb, E., & Ekpe, E.-O. I. (2017). Cyber security in the Nigerian banking sector: An appraisal of audit committee effectiveness. *International Review of Management and Marketing, 7*(2), 340–346.

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology.

Pfeffer, J., & Salancik, G. R. (1978). The external control of organizations: A resource dependence perspective. Harper & Row.

Quinn, S., Pascoe, C., Barrett, M., Scarfone, K., & Witte, G. (2024). NIST Cybersecurity Framework 2.0: Quick-start guide for using the CSF tiers (NIST Special Publication 1302). National Institute of Standards and Technology.

Smith, J. L., et al. (2021). Cybersecurity breaches and the role of information technology governance in audit committee charters. *Journal of Information Systems, 35*(1), 101–119.

World Economic Forum. (2024). Global cybersecurity outlook 2024. World Economic Forum.