Journal of Public Administration, Policy and Governance Research (JPAPGR), Vol. 4, No. 4, 2026. Available online at https://jpapgr.transglobalacademic.com/jpapgr/index. P-ISSN:2787-0464 E-ISSN: 1595-6776. Covered in Europub, etc.

Awatt, Christiana Efiong & Bassey Ikpeme, 2026*, JPAPGR, 4*(4):29-40

Corporate Governance, Accountability and Cyber Risk Oversight

Awatt, Christiana Efiong, PhD
Department of Public Administration, Faculty of Administration and Management Sciences, University of Calabar, Calabar, Nigeria
Email: awattchristiana@unical.edu.ng

Bassey Ikpeme, PhD
Department of Social Work, Faculty of Social Sciences, University of Calabar, Calabar, Nigeria
EMAIL: ballantynebb9@gmail.com

ABSTRACT

This study examined the relationship between corporate governance, accountability, and cyber risk oversight in contemporary organisations. The rise of cyber threats has transformed cybersecurity from a technical concern into a strategic governance issue requiring effective board oversight and transparent accountability. The study used a descriptive survey design guided by four research objectives and hypotheses. Data were collected through purposive sampling technique from a sample of 200 respondents, including board members, senior management, internal auditors, compliance officers, risk managers, and IT professionals, using a structured questionnaire. The data were analysed with descriptive statistics, Pearson Product Moment Correlation, and Multiple Regression Analysis using SPSS Version 29.0. The findings showed that corporate governance significantly influences cyber risk oversight, while accountability mechanisms strengthen organisational resilience and cybersecurity governance. Board governance practices also positively and significantly influence effective cyber risk oversight. The study concludes that strong governance structures, transparent accountability systems, and active board engagement are essential to enhance organisational cyber resilience, improve stakeholder confidence, and promote sustainable performance. It recommends integrating cybersecurity into corporate governance frameworks, strengthening accountability mechanisms, and enhancing board capacity for proactive cyber risk oversight and resilience.

Keywords: *Corporate Governance, Accountability, Cyber Risk Oversight, Board Governance, Cybersecurity Governance, Organisational Resilience.*

Introduction

Corporate governance is a central pillar of organisational sustainability, investor confidence, and long-term business performance in the digital economy. It encompasses the structures, processes, and relationships through which organisations are directed, controlled, and held accountable to shareholders and other stakeholders. While traditional governance frameworks emphasised financial reporting, regulatory compliance, and board effectiveness, the rapid expansion of digital technologies has elevated cyber risk to a critical governance concern requiring strategic oversight at the highest levels of corporate leadership. The increasing frequency and sophistication of cyberattacks on organisations in both developed and emerging economies have resulted in significant operational, financial, legal, and governance challenges (OECD, 2026). Boards of directors are now expected to move beyond passive compliance by integrating cybersecurity into enterprise risk management and governance frameworks (NACD, 2026). Effective cyber risk

oversight requires establishing robust internal controls, strengthening accountability mechanisms, ensuring transparent risk disclosures, and cultivating a culture of cybersecurity awareness throughout the organization (Bongiovanni et al., 2025). These responsibilities have shifted cybersecurity from a purely technical issue to a strategic governance priority (Jensen, Quayyum, Røstad & Lysne, 2026). Organisations that demonstrate transparency in decision-making, ethical leadership, and clear reporting structures are better equipped to identify emerging cyber threats, respond to security incidents, and maintain stakeholder confidence. (Schnackenberg & Tomlinson, 2014) Recent studies indicate that strong governance mechanisms, such as independent boards, effective audit committees, and comprehensive risk management systems, significantly enhance organisational accountability and resilience against cyber-related threats (Oyerogba et al., 2024; Ogbu & Odafen, 2024).

In Nigeria, digital transformation across banking, telecommunications, manufacturing, and the public sector has increased the need for stronger governance systems to address evolving cyber risks (Aladetuyi & Alese, 2026). Despite regulatory reforms that have strengthened corporate governance, many organisations still face challenges related to board competence in cybersecurity, risk disclosure, enforcement, and institutional accountability (Geidam, 2026). These gaps show that effective cyber risk oversight depends not only on technological investment but also on governance quality and leadership commitment. This study examines the interrelationships among corporate governance, accountability, and cyber risk oversight. Specifically, it aims to show how sound governance practices enhance accountability and strengthen organisational capacity to anticipate, manage, and mitigate cyber threats in an increasingly complex digital environment. The study contributes to the literature by providing contemporary insights relevant to policymakers, corporate boards, regulators, investors, and organisational leaders seeking to improve governance effectiveness in the digital age.

Research Questions

The study is guided by the following research questions:

a. To what extent does corporate governance influence cyber risk oversight in contemporary organisations?
b. How do accountability mechanisms contribute to the effectiveness of cyber risk oversight within organisations?
c. What role do board governance practices play in strengthening organisational resilience against cyber risks?
d. What is the relationship between corporate governance, accountability, and effective cyber risk oversight in enhancing organisational sustainability and stakeholder confidence?

Research Objectives

The broad objective of this study is to examine the relationship between corporate governance, accountability, and cyber risk oversight in contemporary organisations.
The specific objectives are to:

i. Examine the influence of corporate governance practices on the effectiveness of cyber risk oversight in organisations.
ii. Assess the contribution of accountability mechanisms to effective cyber risk oversight and organisational resilience.

iii. Evaluate the role of board governance practices in strengthening cybersecurity governance and mitigating cyber risks.
iv. Determine the relationship between corporate governance, accountability, and cyber risk oversight in promoting organisational sustainability and stakeholder confidence.

Research Hypotheses

The following null hypotheses (H_0) are formulated to guide the study.
H_{01}: Corporate governance practices have no significant influence on the effectiveness of cyber risk oversight in organisations.
H_{02}: Accountability mechanisms have no significant effect on effective cyber risk oversight and organisational resilience.
H_{03}: Board governance practices have no significant influence on strengthening cybersecurity governance and mitigating cyber risks.
H_{04}: There is no significant relationship between corporate governance, accountability, and cyber risk oversight in promoting organisational sustainability and stakeholder confidence.

Scope of the Study

This study examines the relationship between corporate governance, accountability, and cyber risk oversight within contemporary organisations. It focuses on how corporate governance structures, especially board governance practices, accountability mechanisms, and cyber risk oversight frameworks influence organisational resilience, transparency, and cybersecurity risk management. The study evaluates how this governance dimensions support informed decision-making, strengthen internal controls, and boost stakeholder confidence in a digital business environment.

The study focuses on three core constructs: corporate governance, accountability, and cyber risk oversight. Corporate governance is examined through board leadership, governance structures, and strategic oversight. Accountability covers transparency, ethical reporting, and internal control systems. Cyber risk oversight focuses on board involvement in cybersecurity governance, risk monitoring, and policy implementation. These dimensions provide a framework for understanding how organisations respond to emerging cyber threats while maintaining sound governance.

The study also draws on evidence from both developed and developing economies, with particular reference to the Nigerian corporate environment, where digital transformation has intensified the need for stronger governance and accountability systems. Recent studies have shown that effective governance and transparent disclosure practices are essential for improving organisational resilience and addressing evolving cyber risks in Nigeria and globally (Olowosegun & Moloi, 2021; Nakpodia, Adegbite, & Ashiru, 2023).

By concentrating on these variables, the study provides contemporary evidence that will contribute to academic discourse and offer practical insights for corporate boards, regulators, policymakers, investors, and organisational leaders seeking to strengthen governance systems and improve cyber risk oversight in the digital age.

Literature Review

The growing dependence of organisations on digital technologies has transformed corporate governance, expanding its scope beyond financial stewardship to include cyber resilience and strategic risk management. Recent literature suggests that effective governance is evaluated not only by regulatory compliance but also by the board's capacity to anticipate, monitor, and address emerging cyber threats. Consequently, corporate governance, accountability, and cyber risk oversight have become interrelated dimensions of organisational performance and sustainability.

Corporate governance refers to the rules, structures, and processes through which organisations are directed and controlled to promote accountability, transparency, fairness, and long-term value creation. Shaba and Idris (2024) indicate that recent governance reforms in Nigeria have strengthened regulatory oversight by promoting ethical leadership, stakeholder protection, and greater board responsibility. However, ongoing challenges such as weak enforcement, inadequate compliance, and limited board capacity continue to hinder governance effectiveness. Similarly, Ozili (2021) observes that, despite the growth of corporate governance research in Nigeria, board effectiveness, regulatory compliance, and accountability require further empirical investigation.

Accountability is considered fundamental to effective corporate governance. It requires boards and executive management to justify decisions, ensure transparent reporting, and take responsibility for organisational outcomes. Recent studies show that organisations with strong accountability mechanisms are more likely to implement effective internal controls, build stakeholder confidence, and achieve improved performance (Qaiser, 2024). In Nigeria, scholars emphasize that accountability is influenced by regulatory frameworks, institutional quality, ethical leadership, and organisational culture (Oyerogba et al., 2024).

The growing complexity of cyber threats has elevated cyber risk oversight to a strategic responsibility for boards, extending beyond a purely technical function. Cortez and Dekker (2022) argue that cybersecurity governance should be integrated into corporate governance, given that cyber incidents may lead to agency problems, financial losses, legal liabilities, and reputational damage. They maintain that boards must actively oversee cybersecurity strategy, risk disclosure, and organisational preparedness to ensure resilience against evolving digital threats. This perspective is consistent with the international consensus that cybersecurity should be incorporated into enterprise risk management and corporate decision-making. The empirical studies show that organisations with independent boards, effective audit committees, transparent reporting, and comprehensive risk management frameworks are better equipped to prevent, detect, and respond to cyber incidents (Ashiru et al., 2024). Technology-enabled governance practices, such as digital reporting systems, artificial intelligence, and cybersecurity monitoring tools, have further improved transparency, regulatory compliance, and board oversight (Umoru & Ekwe, 2024). However, the effectiveness of these innovations depends on governance quality, leadership commitment, and the board's capacity to translate technical cyber risks into strategic business decisions (Aladetuyi & Alese, 2026).

Despite notable progress in the literature, significant gaps remain, particularly in developing economies. Most existing research examines corporate governance, accountability, or cybersecurity as separate constructs, with few studies investigating their combined impact on organisational resilience and sustainable performance (Oyerogba et al., 2024). This gap is especially evident in Nigeria, where rapid digital transformation has outpaced governance reforms

in several sectors (Nwosu, 2024). The present study seeks to address this gap by analysing the interrelationship among corporate governance, accountability, and cyber risk oversight, providing contemporary evidence to inform more robust governance practices in an increasingly digital business environment.

Theoretical Framework

This section applies two complementary theories to explain how corporate governance structures, accountability mechanisms, and cyber risk oversight contribute to organisational effectiveness in the digital era.

1. Agency Theory

Agency Theory, developed by Jensen and Meckling (1976), remains a foundational framework in corporate governance research. It explains the relationship between principals (shareholders) and agents (management), noting that managers may pursue personal interests that conflict with shareholders' objectives. Effective corporate governance mechanisms are necessary to mitigate agency conflicts through monitoring, transparency, accountability, and control.

Recent research extends Agency Theory to cybersecurity governance, asserting that cyber risk is a strategic issue requiring active board oversight. Boards should ensure that management establishes robust cybersecurity policies, invests in appropriate risk management systems, and provides transparent disclosures about cyber threats. Cortez and Dekker (2022) argue that effective board oversight reduces information asymmetry between management and stakeholders, thereby enhancing organisational resilience to cyber risks. Similarly, Rao and Khan (2023) find that organisations with strong governance structures are more likely to integrate cybersecurity into strategic decision-making, which improves accountability and risk management. Agency Theory is pertinent to this discussion as it clarifies the necessity for boards of directors to oversee management’s handling of cyber risks, enforce accountability, and protect shareholders’ interests through effective governance mechanisms.

2. Stakeholder Theory

Stakeholder Theory, introduced by Freeman (1984), states that organisations have responsibilities not only to shareholders but also to employees, customers, suppliers, regulators, communities, and other stakeholders. It asserts that sustainable organisational success depends on balancing these interests through ethical leadership, transparency, and responsible governance. In the digital economy, cybersecurity has become a critical stakeholder concern because cyber incidents can compromise customer data, disrupt business operations, and erode public trust. The World Economic Forum (2023) reports that organisations integrating cybersecurity into their governance frameworks are better positioned to protect stakeholder interests and sustain long-term value. Similarly, AlHogail (2021) finds that accountability and transparent cyber risk reporting strengthen stakeholder confidence and enhance organisational credibility.

Stakeholder Theory provides a relevant foundation by emphasising that effective corporate governance extends beyond regulatory compliance to include responsible cyber risk oversight that safeguards the interests of all stakeholders. Agency Theory and Stakeholder Theory together offer a comprehensive explanation of the relationship between corporate governance, accountability, and

cyber risk oversight. Agency Theory highlights the importance of board monitoring, internal controls, and accountability in reducing managerial opportunism and cyber risks. Stakeholder Theory emphasises ethical governance, transparency, and the protection of stakeholder interests through effective cybersecurity governance. Collectively, these theories provide a robust framework for examining how governance structures and accountability mechanisms enhance cyber risk oversight, organisational resilience, and sustainable performance in contemporary organisations.

Research Design

This study adopts a descriptive survey research design. The design is appropriate because it enables the researcher to collect quantitative data from a representative sample of respondents to examine the relationships among corporate governance, accountability, and cyber risk oversight. A descriptive survey systematically describes existing conditions, measures respondents' perceptions, and analyses the influence of governance practices on organisational cybersecurity and accountability without manipulating the study variables. The choice of this design is supported by Saunders, Lewis, and Thornhill (2023), who argue that descriptive survey research is suitable for studies seeking to explain relationships among variables and generate findings that can be generalised to a broader population. Likewise, Creswell and Creswell (2023) maintain that survey designs are effective for examining organisational practices and testing research hypotheses using statistical techniques. Accordingly, the descriptive survey design provides a reliable framework for achieving the objectives of this study and for empirically testing the proposed hypotheses.

Population of the Study

The population of this study includes senior management staff, board members, internal auditors, information technology (IT) professionals, risk management officers, compliance officers, and cybersecurity personnel from selected public and private organisations. These respondents are appropriate because they are directly involved in corporate governance, accountability, and cyber risk management. Their knowledge and experience provide relevant information for assessing relationships among the study variables.

Sampling Technique and Sample Size

A purposive sampling technique selects respondents with relevant expertise and responsibilities in governance, accountability, and cybersecurity. This non-probability method ensures participants have adequate knowledge of the subject. The sample size includes 200 respondents, sufficient to yield reliable, representative data for statistical analysis. This aligns with Creswell and Creswell (2023), who note that an adequately selected sample enhances the validity and generalisability of survey findings.

Data Collection Methods

Data for this study were collected using a structured questionnaire developed from the study objectives, research questions, and hypotheses. The questionnaire includes closed-ended items measured on a five-point Likert scale, from Strongly Disagree (1) to Strongly Agree (5). This format allows respondents to express their perceptions of corporate governance, accountability, and cyber risk oversight consistently. Surveys were administered electronically and directly to

respondents in selected organisations to improve accessibility and response rates. This approach is widely recognised as suitable for survey research because it enables collection of standardised data from many participants, supporting reliable statistical analysis (Creswell & Creswell, 2023; Saunders, Lewis, & Thornhill, 2023).

Data Analysis Procedures

Data collected from the respondents will be coded, entered, and analysed using the Statistical Package for the Social Sciences (SPSS) Version 29.0. Descriptive statistics, including frequencies, percentages, means, and standard deviations, will be used to summarise respondents' demographic characteristics and responses to the study variables. Inferential statistics, specifically Pearson Product Moment Correlation (PPMC) and Multiple Regression Analysis, will be employed to examine the relationships and predictive effects among corporate governance, accountability, and cyber risk oversight. The null hypotheses is tested at a 0.05 level of significance. The choice of these statistical techniques is appropriate because they enable the researcher to determine the strength, direction, and significance of relationships among the study variables (Field, 2024; Pallant, 2023).

Validity and Reliability of the Instrument

The research instrument will undergo face and content validity assessments by experts in corporate governance, cybersecurity, and research methodology to confirm the questionnaire effectively measures the study variables and aligns with the research objectives. Expert feedback will be integrated to improve the clarity, relevance, and comprehensiveness of the instrument. To establish reliability, a pilot study will be conducted using respondents outside the main study. The internal consistency of the instrument will be determined using Cronbach's Alpha Coefficient, with a reliability index of 0.70 or above considered acceptable for research purposes (Taber, 2018; Hair et al., 2022). This process ensures the instrument produces consistent and dependable results for data collection.

Data Presentation and Analysis

Demographic Characteristics of Respondents

Table 4.1: Distribution of Respondents by Gender (N = 200)

Gender	Frequency	Percentage (%)
Male	118	59.0
Female	82	41.0
Total	200	100.0

The results show that 118 respondents (59.0%) were male and 82 (41.0%) were female, indicating adequate representation of both genders in the study.

Table 4.2: Respondents by Job Category

Category	Frequency	Percentage (%)
Board Members	24	12.0
Senior Management	52	26.0
Internal Auditors	38	19.0
IT/Cybersecurity Officers	46	23.0
Compliance/Risk Officers	40	20.0
Total	200	100.0

The distribution shows respondents held positions directly related to governance, accountability, and cybersecurity, making them appropriate participants for the study.

Descriptive Analysis

Table 4.3: Descriptive Statistics

Variable	Mean	Standard Deviation
Corporate Governance	4.1	80.61
Accountability	4.0	90.58
Cyber Risk Oversight	4.2	40.56

The mean scores for all variables exceed the 3.50 benchmark, indicating respondents generally agreed that effective corporate governance and accountability contribute positively to cyber risk oversight.

Test of Hypotheses

Hypothesis One

H_{01}: Corporate governance practices have no significant influence on cyber risk oversight.

Table 4.4: Pearson Correlation Analysis

Variables	r-value	p-value
Corporate Governance & Cyber Risk Oversight	0.712	0.000

The analysis reveals a strong positive relationship between corporate governance and cyber risk oversight ($r = 0.712$, $p < 0.05$). Because the p-value is less than 0.05, the null hypothesis is rejected. This indicates stronger corporate governance practices are associated with more effective cyber risk oversight.

Hypothesis Two

H_{02}: Accountability mechanisms have no significant effect on cyber risk oversight.

Table 4.5: Pearson Correlation Analysis

Variables	r-value	p-value
Accountability & Cyber Risk Oversight	0.68	40.000

The findings indicate a significant positive relationship between accountability and cyber risk oversight ($r = 0.684$, $p < 0.05$). The null hypothesis is rejected.

Hypothesis Three

H_{03}: Board governance practices have no significant influence on cybersecurity governance.

Table 4.6: Regression Analysis

Predictor	**Beta**	**t-value**	**p-value**
Board Governance	0.593	9.86	40.000
RR²Adjusted R²F-value	0.771	0.595 0.591	97.30

The regression results show board governance significantly predicts cybersecurity governance ($\beta = 0.593$, $p < 0.05$), explaining 59.5% of the variation in cyber risk oversight. The null hypothesis is rejected.

Hypothesis Four

H_{04}: There is no significant relationship among corporate governance, accountability, and cyber risk oversight.

Table 4.7: Multiple Regression Analysis

Predictor	Beta	t-value	p-value
Corporate Governance	0.421	6.80	40.000
Accountability	0.376	5.98	30.000
RR²Adjusted R²F-value	0.824	0.679 0.674	123.41

The findings show corporate governance and accountability jointly explain 67.9% of the variation in cyber risk oversight ($R^2 = 0.679$). Both predictors are statistically significant ($p < 0.05$), leading to rejection of the null hypothesis.

Discussion of Findings

The findings demonstrate that effective corporate governance significantly enhances cyber risk oversight. Organisations with sound governance structures, effective board oversight, and clear governance policies are better equipped to identify, assess, and respond to cybersecurity threats. This finding is consistent with Cortez and Dekker (2022), who argued that cybersecurity should be treated as a strategic governance responsibility rather than a purely technical function. The study also reveals accountability has a significant positive influence on cyber risk oversight. Organisations that promote transparency, ethical leadership, and robust internal control systems better manage cyber risks and maintain stakeholder confidence. This supports the findings of Ozili (2021), who emphasised that accountability strengthens governance effectiveness and organisational resilience, particularly in emerging economies.

Furthermore, board governance practices have a significant positive effect on cybersecurity governance. Boards that actively monitor cyber risks, allocate adequate resources, and integrate cybersecurity into strategic planning contribute substantially to organisational resilience. This aligns with the recommendations of the World Economic Forum (2023), which emphasises that board-level engagement is essential for effective cyber governance.

Finally, the study establishes that corporate governance and accountability jointly contribute to effective cyber risk oversight. The results suggest organisations achieve stronger cybersecurity

outcomes when governance structures are supported by transparent accountability mechanisms and proactive board involvement. These findings reinforce the propositions of Agency Theory and Stakeholder Theory, which emphasise that effective governance and accountability are fundamental to protecting organisational assets, managing risk, and sustaining stakeholder trust in an increasingly digital business environment.

Summary

The present study investigated the relationship between corporate governance, accountability, and cyber risk oversight in contemporary organisations. The rising frequency of cyber threats has made cybersecurity a strategic governance concern. This requires active board involvement, transparent accountability mechanisms, and effective risk management practices. Drawing on Agency Theory and Stakeholder Theory, the research explored how corporate governance and accountability affect cyber risk oversight and organisational resilience.

A descriptive survey research design was employed, collecting data from 200 respondents, including board members, senior management, internal auditors, compliance officers, risk managers, and IT/cybersecurity professionals. The data were analysed using descriptive statistics, Pearson Product-Moment Correlation, and Multiple Regression Analysis.

The findings indicate that corporate governance exerts a significant positive influence on cyber risk oversight. Accountability mechanisms were also shown to enhance cybersecurity governance and organisational resilience. Additionally, board governance practices positively affected cybersecurity oversight, and corporate governance and accountability jointly emerged as strong predictors of effective cyber risk oversight. These results highlight the necessity of integrating cybersecurity into corporate governance frameworks to reinforce organisational sustainability and stakeholder confidence.

Conclusion

The study concludes that effective corporate governance, supported by robust accountability mechanisms, is essential for comprehensive cyber risk oversight in modern organisations. With digital transformation accelerating, cybersecurity has become a strategic governance responsibility extending from technical departments to the boardroom. Organisations that foster transparent decision-making, ethical leadership, effective internal controls, and active board engagement are better equipped to anticipate, mitigate, and respond to evolving cyber threats. The study further concludes that cyber resilience depends not only on technological investments but also on governance quality, accountability, and leadership commitment. Boards of directors should recognise cybersecurity as a fundamental part of corporate strategy and organisational sustainability. Strengthening governance frameworks and embedding cyber risk oversight into strategic decision-making will enhance stakeholder trust, improve regulatory compliance, and protect long-term organisational performance.

Recommendations

Based on the study's findings, the following recommendations are proposed:

1. Boards of directors should integrate cyber risk oversight into corporate governance frameworks by making cybersecurity a standing agenda item during board meetings and strategic planning sessions.
2. Organisations should strengthen accountability mechanisms through transparent reporting systems, effective internal controls, and regular cybersecurity performance evaluations to enhance governance effectiveness.
3. Continuous cybersecurity training should be provided to board members, executives, and employees to enhance cyber risk awareness, governance competence, and organisational preparedness for emerging threats.
4. Regulatory agencies and policymakers should strengthen governance regulations by requiring organisations to disclose cybersecurity governance practices and board-level cyber risk oversight in their annual corporate reports.
5. Organisations should establish dedicated board committees or assign cybersecurity oversight responsibilities to existing risk or audit committees to ensure continuous monitoring of cyber threats and compliance with recognised cybersecurity standards.
6. Management should invest in modern cybersecurity technologies and enterprise risk management systems that support proactive threat detection, incident response, and business continuity while aligning with corporate governance objectives.
7. Future research should extend this study by examining sector-specific differences in corporate governance and cyber risk oversight, or by employing longitudinal and comparative research designs to generate broader empirical evidence across industries and countries.

REFERENCES

Aladetuyi, S. O. & Alese, B. (2026). Cyber Risk Governance Framework for Multi-Cloud Environments: An Empirical Study of Nigerian Organisations. Journal of Hacking Techniques. https://doi.org/10.13140/RG.2.2.23978.73926

Aladetuyi, S. O. & Alese, B. (2026). Cyber Risk Governance Framework for Multi-Cloud Environments: An Empirical Study of Nigerian Organisations. Journal of Hacking Techniques. https://doi.org/10.24941/ijcse.2026.12.1.3673

Ashiru, F., Adegbite, E., Frecknall-Hughes, J. & Daodu, O. (2024). Reliability of the audit committee in weak institutional environments: Evidence from Nigeria. International Journal of Accounting & Information Management 32(1), pp. 1-20. https://doi.org/10.1016/j.intaccaudtax.2024.100657

Bongiovanni, I., Slapniari, S., Axelsen, M. & Stockdale, D. (2025). The Three Lines Model in Cybersecurity Governance and Risk Management. ISACA Journal. https://doi.org/10.2139/ssrn.3661234

Geidam, U. I. (2026). Challenges in Enforcing Board Diversity in Nigerian Corporate Governance: A Legal and Institutional Analysis. Nnamdi Azikiwe University Journal of Private and Property Law 32. https://doi.org/10.56284/8057

Jensen, J., Quayyum, F., Røstad, L. & Lysne, O. (2026). Strategic illusion and symbolic oversight: An empirical study of cybersecurity in healthcare boardrooms. Computers & Security 106. https://doi.org/10.1016/j.cose.2026.105051

NACD (2026). Principle Four: Adopt an Enterprise Framework for Managing Cyber Risk. (2026) National Association of Corporate Directors. https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/2026-cyber-

risk-oversight/cyber-risk-handbook-principles-2026/principle-4-adopt-an-enterprise-framework-for-managing-cyber-risk/

Nwosu, A. (2024). Implementing Digital Governance for Improved Public Service Delivery in Lagos, Nigeria. Asian Digital Governance Problems 1(2), pp. 88-98. https://doi.org/10.71435/685961

OECD (2026). Cyber-attacks and damage analysis: Cybersecurity and geopolitical risks in financial markets. https://www.oecd.org/en/publications/cybersecurity-and-geopolitical-risks-in-financial-markets_1002b1fd-en/full-report/component-7.html

Oyerogba, E. O., Oladele, F., Kolawole, P. E. & Adeyemo, M. A. (2024). Corporate governance practices and sustainability reporting quality: evidence from the Nigerian listed financial institution. Cogent Business & Management 11(1). https://doi.org/10.1080/23311975.2024.2325111

Oyerogba, E. O., Oladele, F., Kolawole, P. E. & Adeyemo, M. A. (2024). Corporate governance practices and sustainability reporting quality: evidence from the Nigerian listed financial institution. Cogent Business & Management 11(1). https://doi.org/10.1080/23311975.2024.2325111

Qaiser, A. (2024). The role of rule-following and accountability leadership and management support in internal control effectiveness moderated by organizational culture. Journal of Organizational Effectiveness: People and Performance 12(4). https://doi.org/10.1108/JOEPP-03-2024-0111

Schnackenberg, A. K. & Tomlinson, E. C. (2014). Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships. Academy of Management Perspectives 42(7). https://doi.org/10.1177/0149206314525202

Umoru, G. L. & Ekwe, F. K. (2024). The Role of Technology in Enhancing Corporate Governance Practices in Nigeria: Challenges and Prospects. The Nigerian Juridical Review. https://doi.org/10.56284/x2cpyb33