A Theoretical Review of Internal Control System on Cyber Risk Management in Nigerian Banks

Atelhe Joy Sekele
Department of Accountancy
University of Cross River State
https://doi.org/10.56201/ijbfr.vol.12.no9.2026.pg21.29

Abstract
The purpose of the study was to examine internal control system on cyber risk management in Nigerian banks. The rapid adoption of digital banking technologies has transformed the Nigerian banking sector, making banking services faster, more accessible and increasingly dependent on interconnected information systems. The study recommended that management of Nigerian banks should strengthen the control environment by demonstrating clear commitment to cybersecurity, establishing accountability for cyber risks and developing an organizational culture that promotes ethical behaviour and security consciousness. Banks should conduct regular cyber-risk assessments covering digital banking platforms, information systems, employees, third-party service providers and emerging cyber threats. Nigerian banks should strengthen access controls, authentication procedures, segregation of duties, transaction authorization, encryption and automated monitoring mechanisms to reduce unauthorized access and fraudulent electronic transactions.

Keywords: *Internal control system, cyber risk management, digital banking technologies*

Introduction

The rapid adoption of digital banking technologies has transformed the Nigerian banking sector, making banking services faster, more accessible and increasingly dependent on interconnected information systems. However, this digital transformation has also exposed banks to growing cyber risks, including phishing, identity theft, malware, ransomware, data breaches and unauthorized electronic transactions. Consequently, effective cyber risk management has become an important component of maintaining financial stability, protecting customer information and sustaining public confidence in the banking system. An effective internal control system provides the structures, policies and procedures through which banks identify, prevent, detect and respond to operational and cyber-related threats. Strong controls such as segregation of duties, authorization procedures, access controls, continuous monitoring, internal audit and risk assessment can reduce the likelihood and impact of cyber incidents. Recent literature emphasizes that organizational controls, governance and technological capabilities are increasingly important in strengthening cybersecurity and organizational resilience (Aldasoro et al., 2022; Basel Committee on Banking Supervision (BCBS), 2023; International Monetary Fund, 2024). In Nigeria, where electronic payments and digital banking continue to expand, strengthening internal control systems is therefore critical to effective cyber risk management and the long-term stability of banks.

Theoretical Framework

The theoretical framework provides the intellectual foundation for examining the relationship between internal control system and cyber risk management in Nigerian banks. The study is anchored primarily on the Control Theory, while the Technology–Organization–Environment (TOE) framework provides complementary support. The selection of these perspectives is appropriate because cyber risk management in modern banking is influenced by both the strength of organizational controls and the technological and environmental conditions under which banks operate.

Control Theory

Control Theory provides the principal theoretical foundation for this study. The theory is concerned with the mechanisms through which organizations regulate behaviour, monitor activities and correct deviations in order to achieve predetermined objectives. In an organizational setting, control mechanisms provide management with the means of ensuring that employees and organizational processes operate within established policies, standards and acceptable risk levels. The relevance of Control Theory to the present study becomes particularly clear in the highly digitized banking environment. Nigerian banks rely extensively on information technology, electronic payment platforms, mobile banking, internet banking and interconnected databases. These technologies create opportunities for efficiency but also expose banks to cyber threats. Consequently, banks require effective control mechanisms to regulate access to information systems, authorize transactions, identify vulnerabilities and monitor activities.

The control environment establishes the tone of the organization by defining management's commitment to integrity, accountability and effective control. Risk assessment enables management to identify and evaluate threats capable of affecting organizational objectives. Control activities translate management policies into specific preventive and detective procedures, while information and communication ensure that relevant risk information reaches the appropriate personnel. Finally, monitoring activities determine whether established controls continue to function effectively. These five components correspond directly with the COSO Internal Control—Integrated Framework. From a cyber-risk perspective, Control Theory suggests that stronger organizational controls should reduce opportunities for unauthorized access, manipulation of information, fraudulent electronic transactions and other cyber-related incidents. This argument is especially important in banking because a weakness in one control area can create vulnerabilities that affect several other organizational processes. Thus, the theory provides a logical basis for examining whether control environment, risk assessment, control activities, information and communication, and monitoring activities influence cyber risk management.

Technology–Organization–Environment (TOE) Framework

The Technology–Organization–Environment (TOE) framework, developed by Tornatzky and Fleischer (1990), provides a complementary perspective for understanding the study. The framework explains how organizational outcomes relating to technology are influenced by three broad contexts: the technological context, organizational context and environmental context. The technological context concerns the technologies available to an organization and their characteristics, including cybersecurity systems, authentication mechanisms, information systems and digital infrastructure. The organizational context covers management support, organizational structure, human resources, policies, organizational capabilities and internal control mechanisms.

The environmental context encompasses external factors such as regulatory requirements, competitive pressures, customers, suppliers and the changing cyber-threat environment. The TOE framework is particularly relevant to Nigerian banks because effective cyber risk management cannot be achieved through technology alone. A bank may possess sophisticated cybersecurity infrastructure but still remain vulnerable if management does not establish appropriate policies, employees lack cybersecurity awareness, responsibilities are unclear or control mechanisms are poorly monitored. The increasing integration of digital technologies into financial services therefore requires banks to consider technological capabilities alongside organizational governance and external environmental pressures.

The contemporary importance of governance in cybersecurity is also reflected in the NIST Cybersecurity Framework 2.0, which places Govern alongside Identify, Protect, Detect, Respond and Recover. NIST (2024) emphasizes that cybersecurity risk management requires organizations to establish governance, assess risks, protect critical assets, detect threats and maintain response and recovery capabilities. This reinforces the argument that cyber risk management involves an interaction between technology, organizational controls and the wider operating environment. The TOE framework is used as a supporting theoretical perspective because cyber risk management in contemporary banking is inherently technological and organizational. It helps explain why the effectiveness of internal controls may depend on the bank's technological capabilities, organizational readiness and external operating environment.

The combination of these perspectives therefore provides a stronger theoretical explanation than relying on either perspective alone. Control Theory explains the internal control mechanisms through which Nigerian banks can regulate and mitigate cyber risks, while the TOE framework explains the technological, organizational and environmental conditions that influence the effectiveness of those mechanisms. Accordingly, the study is theoretically premised on the assumption that effective internal control mechanisms, supported by appropriate technological capabilities and favourable organizational and environmental conditions, enhance the ability of Nigerian banks to identify, prevent, detect, respond to and recover from cyber risks. This position is consistent with contemporary cybersecurity risk-management thinking, which treats governance, risk identification, protection, detection, response and recovery as interconnected elements of cyber resilience.

Literature Review

Control Environment and Cyber Risk Management

Control environment refers to the organizational conditions, leadership commitment, ethical values, governance structures and management attitudes that establish the foundation for internal control. According to Abdullahi and Mansor (2021), management commitment to internal control significantly influences the effectiveness of organizational mechanisms for preventing and detecting irregularities. In the context of cybersecurity, this dimension is particularly important because employees often constitute an important point of vulnerability within banking information systems. Hadlington (2021) argues that employees' cybersecurity behaviour is strongly influenced by organizational culture, management expectations and security awareness. Similarly, Bada et al. (2022) observed that cybersecurity should not be treated exclusively as a technological issue because organizational culture and employee behaviour significantly affect cyber-risk exposure.

A strong control environment therefore creates a culture in which employees understand their cybersecurity responsibilities and management demonstrates commitment through adequate

policies, resources and accountability mechanisms. Aldasoro et al. (2022) further note that cyber incidents can generate broader operational and financial consequences for financial institutions, making governance and organizational preparedness essential. For Nigerian banks, a strong control environment can consequently provide the foundation for effective cyber risk management by ensuring that cybersecurity responsibilities are clearly defined and supported by senior management.

Risk Assessment and Cyber Risk Management

Risk assessment involves the identification, analysis and evaluation of risks capable of affecting organizational objectives. In banking, effective risk assessment is particularly relevant because cyber threats continuously evolve in form, scale and sophistication. Shetty et al. (2022) explain that organizations need systematic approaches to identify vulnerabilities and assess the potential consequences of cybersecurity threats before determining appropriate responses. Similarly, Aldasoro et al. (2022) emphasize that cyber risk has become an important component of operational risk within financial institutions because disruptions to information systems can affect both individual institutions and the wider financial system. The importance of continuous cyber risk assessment is further supported by Kou et al. (2021), who argue that the identification and evaluation of cyber threats are essential for developing effective risk-management strategies. Rather than waiting for an attack to occur, banks need to regularly examine their systems, digital channels, third-party relationships and employee practices for potential weaknesses. Eling and Schnell (2022) also emphasize that cyber risk assessment is complicated by the constantly changing nature of cyber threats and the difficulty of accurately predicting their frequency and financial consequences. Nigerian banks can therefore improve cyber risk management by incorporating regular cyber-risk assessments into their broader enterprise risk-management processes.

Control Activities and Cyber Risk Management

Control activities are the policies, procedures and mechanisms established by management to ensure that identified risks are appropriately controlled. Within banking institutions, these activities may include authorization procedures, segregation of duties, access restrictions, authentication, transaction verification, encryption and system-based controls. Müller et al. (2023) emphasize that technological controls are important for reducing unauthorized access and protecting critical organizational information resources. Likewise, Tøndel et al. (2021) identify access control and security procedures as important mechanisms for reducing cybersecurity vulnerabilities within organizations. The effectiveness of control activities becomes more significant as banks increasingly depend on electronic and mobile banking platforms. According to Aldasoro et al. (2022), operational disruptions arising from cyber incidents can affect financial institutions' ability to provide essential services. Effective control activities can reduce opportunities for unauthorized transactions, data manipulation and system compromise. Bouveret (2021) similarly identifies cybersecurity and operational resilience as important considerations for financial institutions because weaknesses in digital systems can create significant financial and operational consequences. Nigerian banks should therefore continuously review and strengthen their control activities to ensure that existing controls remain effective against emerging cyber threats.

Information and Communication and Cyber Risk Management

Information and communication concern the processes through which relevant information is identified, processed and communicated to appropriate individuals within an organization. Effective cyber risk management requires timely communication between management, information technology personnel, internal auditors, risk managers and other employees. Bada et al. (2022) argue that cybersecurity awareness and effective communication are essential because employees need to understand the nature of cyber threats and the appropriate actions to take when threats are identified. Similarly, Hadlington (2021) found that employees' cybersecurity behaviour is influenced by their knowledge, awareness and understanding of organizational security expectations. This suggests that even sophisticated technological controls may be weakened where employees do not receive adequate information about cyber threats. Parsons et al. (2021) also emphasize the importance of cybersecurity awareness and behaviour in strengthening organizational security. For Nigerian banks, effective information and communication can facilitate rapid reporting of suspicious activities, improve employee awareness and reduce delays in responding to cyber incidents.

Monitoring Activities and Cyber Risk Management

Monitoring activities involve the continuous and periodic evaluation of internal controls to determine whether they remain effective. In cyber risk management, monitoring is necessary because cyber threats and attack techniques change rapidly. Eling and Schnell (2022) note that the dynamic nature of cyber risk makes continuous assessment and review particularly important for organizations seeking to maintain resilience. Monitoring enables banks to identify weaknesses in their control systems before those weaknesses are exploited. Internal audit also plays an important role in monitoring the effectiveness of internal controls. Eulerich et al. (2022) emphasize the increasing importance of internal audit in evaluating risk-management and control processes as organizations become more digitally dependent. In the banking environment, continuous monitoring can include security-log reviews, system surveillance, vulnerability assessments, internal audit examinations and periodic testing of cybersecurity controls. Aldasoro et al. (2022) further indicate that resilience requires financial institutions to develop capabilities that enable them to withstand and recover from operational disruptions. Nigerian banks that maintain effective monitoring mechanisms are therefore better positioned to detect control weaknesses, respond promptly to cyber threats and strengthen their overall cyber resilience.

Empirical Literature

Empirical evidence has increasingly established a relationship between internal control mechanisms and the management of risks confronting banking institutions, particularly as banking operations become more digitally driven. Ozuomba, Ibeaja, and Nosiri (2023) examined the effect of internal control activities and risk assessment on the operations of quoted banks in Nigeria using data from 16 quoted banks covering 2013–2020. Employing pooled OLS, fixed-effects and random-effects models, the study found that internal control activities had an inverse relationship with operational risk, while risk assessment significantly influenced operational risk. The authors emphasized the need for sustained internal checks, compliance with banking policies and adequate training of internal-control personnel, particularly IT personnel. These findings demonstrate that internal control mechanisms can influence the level of risk experienced by Nigerian banks and provide an important foundation for extending the analysis from general operational risk to the

more contemporary issue of cyber risk. Building on this evidence, Oyebisi (2024) investigated risk management and internal control systems among selected deposit money banks in Lagos State, Nigeria. Using questionnaire data obtained from 122 respondents and multiple regression analysis, the study found that risk management and internal control systems had a positive and significant relationship with the performance and operations of the selected banks. The study further identified risk-monitoring mechanisms and risk-management policies as important factors in ensuring effective risk management and internal control. Although the study was not specifically focused on cybersecurity, its findings suggest that effective internal control and continuous monitoring can strengthen the overall risk-management capacity of Nigerian banks. This is relevant to the present study because cyber risk represents an increasingly important category of risk within the contemporary banking environment. More directly related to cybersecurity, Azura, Azad, and Ahmed (2025) developed an integrated cybersecurity risk-management framework for online banking systems. Their study recognized that the increasing adoption of online banking creates significant security and privacy challenges, including data breaches, exposure of sensitive financial information and operational disruptions. The proposed framework incorporated threat identification, vulnerability analysis, risk assessment, risk treatment and continuous monitoring, while also considering technological and human factors within the banking environment. The study therefore reinforces the argument that effective cyber risk management requires a systematic process of identifying and assessing threats and continuously monitoring the effectiveness of risk controls. However, unlike the present study, the research was primarily concerned with developing an integrated cybersecurity framework rather than empirically examining how specific internal-control dimensions influence cyber risk management in Nigerian banks.

More recent Nigerian evidence provides a much closer relationship to the present study. Nweke and Ekpeh (2026) empirically investigated internal control weaknesses and cybersecurity breach frequency in listed deposit money banks in Nigeria. Using a survey design and least-squares regression, the researchers found a significant positive relationship between internal control weaknesses and cybersecurity breach frequency at the 1% level of significance. The study concluded that weaknesses in internal control systems contribute to increased cybersecurity breaches and recommended stronger management commitment, segregation of duties, automated controls, regular audits and a stronger organizational culture of compliance. This finding provides direct empirical support for the argument that the strength of internal controls is an important determinant of cybersecurity outcomes in Nigerian banks.

Similarly, Abdulkadir and Bello (2026) examined the impact of internal control systems on cybercrime prevention among deposit money banks in Nigeria. The study adopted a descriptive survey design and obtained 138 usable responses from 150 questionnaires administered to bank employees. Using correlation and regression analysis, the researchers found that the five major components of internal control—control environment, risk assessment, control activities, information and communication, and monitoring—were positively and significantly associated with cybercrime prevention. The study is particularly important to the present research because its dimensions correspond closely with those adopted in this study.

Ozuomba et al. (2023) established the relevance of control activities and risk assessment to operational risk; Oyebisi (2024) demonstrated the importance of risk management, monitoring and internal control systems in Nigerian banks; Azura et al. (2025) emphasized systematic cybersecurity risk identification, assessment and continuous monitoring in online banking; while Nweke and Ekpeh (2026) and Abdulkadir and Bello (2026) provided more direct evidence that

internal-control weaknesses are associated with cybersecurity breaches and that the major components of internal control contribute significantly to cybercrime prevention.

Conclusion and Recommendations

An effective internal control system provides the structures, policies and procedures through which banks identify, prevent, detect and respond to operational and cyber-related threats. Strong controls such as segregation of duties, authorization procedures, access controls, continuous monitoring, internal audit and risk assessment can reduce the likelihood and impact of cyber incidents. The study recommended thus:

1. Management of Nigerian banks should strengthen the control environment by demonstrating clear commitment to cybersecurity, establishing accountability for cyber risks and developing an organizational culture that promotes ethical behaviour and security consciousness.
2. : Banks should conduct regular cyber-risk assessments covering digital banking platforms, information systems, employees, third-party service providers and emerging cyber threats. The results should guide management's cybersecurity investment and risk-response decisions.
3. Nigerian banks should strengthen access controls, authentication procedures, segregation of duties, transaction authorization, encryption and automated monitoring mechanisms to reduce unauthorized access and fraudulent electronic transactions.
4. Banks should improve internal communication concerning cybersecurity threats and establish clear procedures for reporting suspicious activities and cyber incidents. Regular cybersecurity awareness programmes should also be provided to employees.

References

Abdulkadir, A., & Bello, [initials]. (2026). The impact of internal control systems on cybercrimes prevention of deposit money banks in Nigeria. *Journal of Business Development and Management Research, 12*(7).

Abdullahi, R., & Mansor, N. (2021). Fraud risk management and internal control effectiveness: Evidence from organizations. *Journal of Financial Crime, 28*(4), 1115–1130.

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). Operational and cyber risks in the financial sector. *BIS Quarterly Review*, 1–15.

Azura, Y. T. Y., Azad, M. A., & Ahmed, Y. (2025). An integrated cyber security risk management framework for online banking systems. *Journal of Banking and Financial Technology*, 9, 85–104. https://doi.org/10.1007/s42786-025-00056-3

Bada, M., Sasse, M. A., & Nurse, J. R. C. (2022). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Journal of Information Security*, 21, 1–15.

Basel Committee on Banking Supervision. (2023). *Principles for operational resilience*. Bank for International Settlements.

Bouveret, A. (2021). Cyber risk for the financial sector: A framework for quantitative assessment. *IMF Working Paper, 2021*(143), 1–33.

Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal control—Integrated framework. COSO.

Eling, M., & Schnell, W. (2022). What do we know about cyber risk and cyber insurance? The Geneva Papers on Risk and Insurance—*Issues and Practice*, 47, 1–23.

Eulerich, M., Kremin, J., & Wood, D. A. (2022). Factors that influence the perceived usefulness of internal audit in the digital age. *Accounting Horizons, 36*(1), 1–20.

Hadlington, L. (2021). Human factors in cybersecurity: Examining the role of individual differences and organizational factors. *Computers & Security*, 105, 102239.

International Monetary Fund. (2024). *Global financial stability report: Steadying the course—Global banking and financial stability*. IMF.

Kou, G., Olgu Akdeniz, Ö., Dinçer, H., & Yüksel, S. (2021). FinTech investments in cybersecurity: A systematic approach. *Technological Forecasting and Social Change,* 167, 120702.

National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Nweke, I. V., & Ekpeh, U. C. (2026). Internal control weaknesses and cybersecurity breach frequency in listed deposit money banks in Nigeria. *IIARD International Journal of Banking and Finance Research, 12*(4). https://doi.org/10.56201/ijbfr.vol.12.no4.2026.pg22.33

Ouchi, W. G. (1979). A conceptual framework for the design of organizational control mechanisms. *Management Science, 25*(9), 833–848. https://doi.org/10.1287/mnsc.25.9.833

Oyebisi, L. O. (2024). Risk management, internal control systems and performance of selected deposit money banks in Lagos State, Nigeria [Master's thesis, Lead City University]. Lead City University Repository.

Ozuomba, C. N., Ibeaja, U. F., & Nosiri, H. U. (2023). Internal control activities and risk assessment effect on the operations of quoted banks in the Nigerian Stock Exchange. *IDOSR Journal of Arts and Management, 8*(1), 27–39. https://doi.org/10.59298/IDOSR/2023/12.1.5893

Parsons, K., Butavicius, M., Pattinson, M., & McCormac, A. (2021). Determining employee awareness and behaviour toward cybersecurity. *Computers & Security*, 109, 102397.

Tøndel, I. A., Jaatun, M. G., & Cruzes, D. S. (2021). Threat modelling and security controls in digital organizations. *International Journal of Information Security*, 20, 1–15.

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.