VOL. 12 NO. 7,
MAY, 2026
E-ISSN 3026-9679
P-ISSN 3026-9423

African Scholar Publications & Research International
www.africanscholarpub.com

Journal of Business Dev. and Management Res. (JBDMR)

The Impact of Internal Control Systems on Cybercrimes Prevention of Deposit Money Banks in Nigeria

Abdul Kerim; G. A. Adebayo (PhD); Sunday Omale (PhD); & Abraham Bello, Monday

Department of Accounting, Faculty of Management and Social Science, Confluence University of Science and Technology, Osara, Kogi State, Nigeria
Corresponding Author: abdulk@custech.edu.ng
DOI: https://doi.org/10.70382/ajbdmr.v12i7.069

Abstract

This study examines the impact of internal control systems on the prevention of cybercrimes in deposit money banks in Nigeria. Against the backdrop of increasing cyber threats and financial fraud, the research sought to determine whether effective internal controls contribute significantly to cybercrime mitigation. A descriptive survey design was adopted, and data were collected using structured questionnaires administered to 150 employees across selected banks. Out of these, 138 responses were analysed using descriptive and inferential statistics, including Pearson correlation and regression analysis. The findings revealed that internal control systems, specifically, the control environment, risk assessment, control activities, information and communication, and monitoring, are positively and significantly associated with the prevention of cybercrimes. The study concludes that robust internal controls are essential in safeguarding banking operations against cyber threats. It recommends strengthening employee training, adopting advanced control technologies, and enhancing monitoring mechanisms to improve cyber resilience. This research contributes to the understanding of internal control effectiveness in the Nigerian banking sector and offers practical guidance for policymakers and practitioners.

Keywords: Internal Control System, Cybercrime Prevention, Deposit Money Banks, Nigeria, Risk Management.

Introduction

In the digital era, the banking industry is increasingly vulnerable to cyber threats due to rapid technological advancements and the growing sophistication of cybercriminals. (Fabiyi, 2025). Deposit Money Banks (DMBs) in Nigeria, which are critical pillars of the country's financial system, have experienced frequent incidents of fraud, phishing attacks, ransomware, identity theft, and unauthorized electronic transfers (Adeleke, 2019). These cybercrimes undermine public confidence, erode profitability, and can destabilize the financial system. A robust internal control system has thus become imperative for mitigating such risks and safeguarding assets. (James & Lucia, 2021)

Fijabi. (2022), see internal control as a procedure or policy put in place by management to safeguard assets, promote accountability, increase efficiency, and prevent fraudulent practices. It has become of primary importance today in Nigerian banks; the reason being that the control system in any organization is a stepping stone for an efficient accounting system (Shehu, 2025). The need for internal control systems in the organization, especially banks, cannot be subverted, because the banking sector, which has a decisive role in the economic development of a nation, is now being characterized by macroeconomic instability, slow growth in economic activities, delinquency, and the risk of fraud (Chukwuemeka, 2025)

A system of internal control is a critical component of bank management and a foundation for the safe and sound operation of deposit money banks in Nigeria. A system of strong internal control can help to ensure that the goals and objectives of deposit money banks are met so that the bank will achieve long-term profitability targets and maintain reliable financial and managerial reporting (Tenbele, 2019). Samuel, (2021), opine that, internal control is not only internal check and internal audit, but the whole system of controls, financial and otherwise, established by the management, to carry on the business of the company in an orderly manner, safeguard its assets and secure as far as possible the accuracy and reliability of its record. A well-founded internal control system, which is always evolving, requires a continuous check and re-checking of day-to-day activities of the business to ensure the correctness and fairness of the accounting records and to detect and expose any deviation when it has occurred (Hudu, 2020). Realizing the importance of an internal control system, a number of metrics have been implemented to improve the services' pertinence by employing the appropriate instruments, methods, personnel, and knowledge to stop and identify fraudulent activity and to ensure the system's pertinence is valuable. Several banks in Nigeria have implemented an internal control system, control environment, risk assessment, information and communication, and monitoring to increase efficiency and reduce fraud cases (Shehu, 2025). Despite all of this work, Nigeria's Deposit Money Banks (DMBs), which operate in a digital banking environment, are increasingly at risk from cybercrimes, which have become more frequent and sophisticated. Nigerian banks still face financial fraud, data breaches, and

illegal access to private client data despite current internal control system frameworks. (Cheng, 2018).

The sufficiency, efficacy, and flexibility of internal control systems in reducing cyber threats are called into question by this enduring vulnerability. Although the goal of internal control systems is to prevent financial misbehavior and encourage operational integrity, there seems to be a gap between their theoretical conception and actual application in the context of cybersecurity. The effectiveness of these controls in stopping cybercrimes may be hampered by elements including a weak enforcement system, an antiquated IT infrastructure, a poor compliance culture, and a lack of employee training. (Abei, 2021).

Statement of Problem

The Nigerian banking industry has undergone rapid digital transformation through electronic banking, mobile banking, internet banking, Automated Teller Machines (ATMs), Point-of-Sale (POS) systems, and real-time payment platforms. While these innovations have improved efficiency, speed and financial inclusion, they have also exposed Deposit Money Banks (DMBs) in Nigeria to increasing cybercrime threats such as phishing, identity theft, malware attacks, hacking, insider fraud, card fraud and unauthorized electronic transfers. Reports from regulatory agencies and financial institutions indicate that cybercrime losses in Nigerian banks have continued to rise despite the presence of internal control frameworks and regulatory guidelines. This trend raises serious concerns about the effectiveness of existing internal control systems in preventing, detecting, and responding to cyber-related fraud.

Internal control systems are expected to provide reasonable assurance regarding the safeguarding of assets, reliability of financial information, compliance with laws, and prevention of fraud. However, many Nigerian banks still experience weak IT governance and inadequate cybersecurity policies, Insider abuse of system privileges, and poor segregation of duties in electronic transactions. Delayed detection of cyber fraud incidents, Inadequate staff awareness and training on cyber risks, and Weak monitoring and auditing of digital transactions. These challenges suggest possible gaps in the design and implementation of internal control systems within Deposit Money Banks. If these gaps persist, customer confidence, financial stability, and the overall integrity of the banking system may be threatened. Despite several studies on fraud and internal control in Nigeria, limited empirical attention has been given specifically to how internal control systems influence cybercrime prevention in Deposit Money Banks. This study, therefore, seeks to examine the impact of internal control systems on cybercrime prevention in Nigerian Deposit Money Banks.

Furthermore, despite becoming more proactive, Nigeria's regulatory environment still lags behind international norms for preventing cybercrime. DMBs are vulnerable to changing cyber threats that could endanger public confidence and financial stability when they rely on antiquated control techniques without incorporating state-of-the-art digital safeguards. In light of this, the study aims to examine how Nigerian deposit money banks' internal control systems,

which include the control environment, risk assessment, and monitoring activities, affect the prevention of cybercrimes**.**

Objectives of the Study

The objective of this study is to examine the impact of internal control systems on the prevention of cybercrimes in Deposit Money Banks in Nigeria for the period of 2019 – 2024. While the Specific Objectives are to:

1. Examine the effect of the control environment on cybercrime prevention in Deposit Money Banks.
2. Assess the impact of risk assessment procedures on cybercrime prevention in Deposit Money Banks.
3. Determine the effect of control activities on cybercrime prevention in Deposit Money Banks.
4. Evaluate the influence of information and communication systems on cybercrime prevention in Deposit Money Banks.
5. Examine the effect of monitoring activities on cybercrime prevention in Deposit Money Banks.

Research Questions

For this study, the study seeks to answer the following questions:

1. To what extent does the control environment influence cybercrime prevention in Deposit Money Banks in Nigeria?
2. How do risk assessment procedures affect cybercrime prevention in Deposit Money Banks?
3. What is the effect of control activities on cybercrime prevention in Deposit Money Banks?
4. How do information and communication systems influence cybercrime prevention in Deposit Money Banks?
5. To what extent do monitoring activities affect cybercrime prevention in Deposit Money Banks?

Research Hypotheses

The hypotheses will be tested in null form:

1. H_{01}: The control environment has no significant effect on cybercrime prevention in Deposit Money Banks in Nigeria.
2. H_{02}: Risk assessment procedures have no significant effect on cybercrime prevention in Deposit Money Banks in Nigeria.
3. H_{03}: Control activities have no significant effect on cybercrime prevention in Deposit Money Banks in Nigeria.
4. H_{04}: Information and communication systems have no significant effect on cybercrime prevention in Deposit Money Banks in Nigeria.

5. H_{05}: Monitoring activities have no significant effect on cybercrime prevention in Deposit Money Banks in Nigeria.

From the above research objectives, research question, and the hypothesis of the study, the findings of this study will provide a practical result that will improve cybersecurity protocols, which could result in measures for boosting internal control systems designed to counter cyberthreats more reliably. Guidelines and Policy Reforms, The Central Bank of Nigeria and other authorities may use the findings to update cybersecurity regulations and DMB internal control specifications. Employee Training Models: In light of the study's findings, banks may implement extensive staff training initiatives centered on incident response, breach prevention, and online safety. Priorities for Technological Investment. Deposit Money Banks (DMBs) will be encouraged by this study to make investments in modern security infrastructure, including multi-layered authentication controls and intrusion detection systems. The time between breach and reaction could be reduced by restructuring compliance units, internal auditing, and improved monitoring frameworks for more proactive threat identification and control testing. The study will set performance standards for institutions for more robust internal controls, enabling others to follow their lead in preventing cybercrime. Increased Public Trust. The general public will become more comfortable utilizing digital banking platforms as a result of apparent advancements in cybersecurity measures, which would be a subtle but significant effect. Lastly, the study will add to the body of knowledge on the intersection of cybersecurity and internal controls in Nigerian financial institutions for scholars and researchers. The remainder of the paper is organized as follows: Section 2 presents relevant extant studies. Section 3 discusses the methodology employed for the study. In section 4, the results of the data analysis are presented and discussed. Section 5 concludes the study by highlighting the findings and their policy implications.

Literature Review

This section examines pertinent research on how internal control mechanisms affect Nigerian deposit money banks' ability to prevent cybercrimes.

Internal control system

Internal control, according to the Committee of Sponsoring Organizations (COSO), is a procedure carried out by the entity's board of directors, management, and other staff members that is intended to give a reasonable level of assurance regarding the accomplishment of goals in terms of operational effectiveness and efficiency, financial reporting reliability, and compliance with relevant laws and regulations (COSO, 2010). Based on this definition, internal controls establish the basis for the amount of work that the professionals in charge of the function must do because they are to protect the organization's funds, guarantee effective and efficient asset management, and ensure that the financial statements are always accurate. It is anticipated that an internal controls system will be able to notify management of possible

issues so that they can be addressed before they become serious issues, though it cannot eliminate all mistakes and anomalies. (Kizil, Kizil, & Dolaz, 2021). Internal controls consist of five integrated components, which include: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. These components provide a framework for managing risks, including those arising from cyber threats. (Shehu, 2025).

Conceptual Review

Control Environment: The control environment encompasses the structure of the organization, the philosophy, style of management, human resources policies, commitment to competence, and the culture of ethical behaviour and communication (Rae & Sands, 2017). In other words, the control environment describes a set of standards, processes, and structures that provide the basis for carrying out internal control across the deposit money banks in Nigeria (Yusuf & Kanji, 2020). The control environment is the bedrock of the COSO Framework because it serves as a foundation for all other internal control components and influences each of the three internal control objectives and all activities (Cheng, 2018). The tone at the top sets the foundation. A culture that prioritizes integrity, accountability, and adherence to security protocols discourages internal fraud and enhances vigilance against external threats. Banks with strong governance frameworks typically invest more in cybersecurity measures and employee awareness.

Risk Assessment: Assessment involves the identification, analysis, and management of uncertainties facing an organization from external and internal sources that threaten the achievement of deposit money banks' objectives (Samuel, 2021). James & Lucia (2021) state that it is meant to identify and analyze relevant risks in the organization, the type of controls required to address the risk, and form a basis for how those risks identified should be managed. In other words, the process encompasses risk identification, risk assessment, and the development of strategies to respond to and mitigate these risks (Wanjala & Riitho, 2020). This, therefore, requires management to consider the impact of possible changes in the internal and external environment to manage the impact (Rae & Sands, 2017). Banks continually assess the likelihood and impact of cyber threats. Through risk assessments, vulnerabilities in IT infrastructure, customer touchpoints, and back-office processes are identified, allowing management to allocate resources to the most critical areas.

Control Activities: Control activities are the policies and procedures established by an organization to ensure that management directives are followed. These encompass a variety of actions, such as authorization and approval processes, segregation of duties to prevent conflicts of interest, and measures to ensure accurate and timely information processing, as it constitutes all actions geared toward helping management, mitigate risks and guarantee the achievement of objectives, (Vutumu ,2024). Control activities are performed at all levels of the entity, at different stages of business processes, including the technology environment, and may be preventive or detective in nature (Munira, 2024). It stipulates the activities needed to

prevent fraud and other risks an organization may face (Riitho & Wanjala, 2020). These are specific policies and procedures designed to mitigate cyber risks. Others include: Segregation of Duties, Access Controls, Encryption, System Reconciliations, and Incident Response Protocols.

Cybercrime and Deposit Money Banks

Zira & Suleiman (2024) assert that Cybercrime refers to a crime in which a computer is the object of the crime or is used as a tool to commit an offense. Cybercriminals may use computer technology to access personal information, business trade secrets, or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication, documents, or data storage. Criminals who perform these illegal activities are often referred to as hackers. Also, Cybercrime can be seen as a computer crime. Cybercrime in the banking sector refers to illegal activities conducted through computer networks to steal funds, manipulate data, or compromise systems. Common forms affecting Nigerian banks include Phishing and social engineering. Hacking into customer accounts. ATM skimming. Insider collusion. Malware attacks on core banking infrastructure (Zira & Suleiman, 2024).

Information, Communication, and Deposit Money Banks

Information and communication include the identification, capture, and exchange of financial, operational, and compliance-related data in a timeframe that allows individuals to fulfill their responsibilities in the attainment of organizational objectives (Abdullah & Barzinji, 2022). Information and communication are critical for conducting, managing, and controlling operations; therefore, the quality of information must be overemphasized. This means that information should be appropriate, timely, reliable, relevant, current, accurate, understandable, and accessible. (Zira & Suleiman, 2024). A robust system ensures that information flows appropriately, internally and externally, supporting informed decision-making and fostering transparency. Continuous communication ensures employees and stakeholders are aware of security policies, incident reporting procedures, and their responsibilities. Regular training reduces the success rate of phishing attacks and social engineering. (Abdullah & Barzinji, 2022).

Monitoring and Deposit Money Banks

Monitoring determines whether all internal control components, including their principles, are in place and functioning as intended. It is a process that is used to evaluate and assess the internal control system of organizations to ensure that it is applied consistently over a long period (Ngigi & Nyakarimi, 2020). In other words, monitoring activities are essential for assessing the ongoing effectiveness of the internal control system. By regularly reviewing and assessing control processes, organizations can identify deficiencies, report them promptly, and take corrective action to maintain and enhance the effectiveness of their internal controls. Abiola (2021) submits that monitoring activities provide information about potential and

actual breakdowns in a control system. Adeleke (2019) posits that the purpose of monitoring is to periodically or systematically determine whether internal control is adequately designed, properly executed, and effective. In other words, all five components of internal control function as designed. Ongoing monitoring through internal audits, surveillance systems, and compliance checks helps identify suspicious activities early. Automated monitoring tools can flag anomalies such as unusual login patterns, large transactions, or unauthorized changes. Monitoring plays a critical role in the performance, stability, and security of Deposit Money Banks (DMBs) in Nigeria. This ensures that internal control systems are functioning as intended, especially in preventing fraud and cybercrimes.

Fraud Triangle Theory

The theory of Fraud Triangle identifies three key factors that must be present in any situation of fraud: perceived threat, incentive, and rationalization. Applied to cybercrimes in Nigerian Deposit Money Banks, it becomes a powerful tool for analysing internal vulnerabilities and shaping control systems. Fraud cannot occur in the absence of the aforementioned elements, and the severity of the fraud would depend on the strength of the elements listed above. Sometimes pressure involves personal circumstances that create a demand for more money; such circumstances could include vices such as drug use or gambling, or simply life events such as a job-losing spouse. Other times, pressure comes from on-the-job problems; unrealistic performance targets can provide the motive for fraud. They may also be non-financial motivators. Opportunity is generated by lax internal controls, poor management supervision, and/or the use of one's position and authority. Chance is the opportunity to overcome regulation over fraud. Rae and Subramanian (2018) warn that incentives relate to an employee's capacity and power to understand and take advantage of the vulnerabilities of the organizational structure by allowing for fraud. Public Accounts Auditor (2011) concluded that the use of one's power and authority to commit fraud occurs on several occasions when internal controls are weak or non-existent, or where there is insufficient management oversight. The chances of committing fraud are improved by reducing the size, resulting in a shortage of workers. The Lebanese Association of Certified Public Accountants (2009) argued that rationalizations involve compensating for being underpaid or substituting a due but not earned bonus. Rationalization is hard to note, since the perpetrator's mind is not understandable. Individuals who commit fraud have a clear mindset to explain or excuse their fraudulent acts (Hooper and Pornelli, 2010).

Perceived pressure for committing fraud in financial institutions

Pressure in case of fraud can be likened to the rationale, that is, what in one’s life steers one to perpetrate fraud. Pressure sometimes presumes personal situations that initiate a demand for more money; such situations might include vices like drug use, gambling, and life events like a spouse losing a job. Subsequently, pressure arises from problems on the job; unrealistic performance targets may provide the motive to perpetrate fraud**.** Motivators can also be non-

financial, like high pressure for good results at work or a need to cover up someone's poor act. Obsessions such as gambling and drugs may also lead someone to perpetrate fraud (Alhassan, 2018).

Opportunity for committing fraud

The Opportunity to commit fraud is feasible when employees have access to assets and information that allows them to both perpetrate and cover up fraud. Employees are given access to records and valuables in the ordinary course of their jobs. Regrettably, that access allows people to perpetrate fraud. Over the recent years, managers have become responsible for a wider range of employees and functions. This has led to more access for them, as well as more control over functional areas of companies. Access must be limited to only those systems, information, and assets that are truly obligatory for an employee to complete his or her job; opportunity is created by weak internal controls, poor management, and/or through the use of one's position and influence. Failure to create adequate policies to detect fraudulent activity also increases the opportunities for fraud to materialize.

Rationalization of committing fraud in financial institutions

There are two facets to rationalization: (1) the fraudster must conclude that the benefits to be realized from a fraudulent activity supersede the possibility of detection. (2)The fraudster needs to substantiate the fraud. Justification can be related to job dissatisfaction or perceived entitlement, or a current intent to make the victim whole sometime in the future, or saving one's family, possessions, or status. Rationalization is discernible by observation of the fraudster's comments or attitudes.

Empirical review

Mohammed and Kabir (2021) studied internal control system effectiveness and fraud prevention in deposit money banks in Nigeria. The study aimed to examine internal control systems and fraud prevention in deposit money banks. The findings of the study showed that there was a positive and significant relationship between the control environment and fraud prevention mechanisms. The overall result showed that control environment, risk assessment, as well as information and communication of internal control, have a positive and significant impact on fraud prevention (Evelyn et al., 2021). Nyakarimi (2015) investigated the internal control system as a means of fraud control in deposit-taking financial institutions in Imenti North Sub-County. The purpose of the study was to establish the relationship between the internal control system and fraud control in deposit-taking financial institutions. The study found that the financial institutions analyzed result through vetting on competencies and integrity, the organizational structure reflects a chain of command, there is proper follow-up of delegated responsibilities, and the employees are promoted and compensated fairly.

A research work conducted by Yolanda (2021) investigated the impact of internal control on fraud detection and prevention in Micro-finance institutions in Cameroon. The results showed

that fraud opportunities were caused as a result of some loopholes in the internal control, such as poor working environment, poor monitoring, low standard facilities, negligence of operations, as well as poor employee recruitment practices. The study shows internal control practices like constant monitoring, fraud training, risk assessment, cash reconciliation, and use of passwords could reduce the fraud opportunity (Abei, 2021).

Kabue and Aduda (2017) investigated the effect of internal controls on fraud prevention among commercial banks in Kenya, where they adopted an explanatory research design while using primary data as the source of data collection. The result indicated there was a negative and significant relationship between reconciliation control and the level of fraud prevention. Research carried out by Cross (2020) in Australia examined how accountability relates to fraud victimization. The purpose of the research was to investigate the general narrative that discerns the way in which responsibility is recognized and the conflict between assigning blame. Analysis showed a high amount of disagreement over who should be held responsible for fraud, including the perpetrator, the victim, and third parties. Findings of research indicated accountability is not controlled by any one party; instead, there seems to be a relationship between victims, perpetrators, and third parties.

Control Environment of Internal Control and Fraud Prevention of Deposit Money Banks in Nigeria

Most sectors across the country have become vulnerable to financial fraud, which could be due to economic hardships, financial scandals, and poor structures against fraud. Control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization (Mulugeta, 2021). James & Lucia (2021) investigated internal control as a tool for fraud control in deposit money banks in Nigeria. The study adopted a survey research design. The test of the hypothesis revealed control environment has a significant contribution towards fraud control in deposit money banks in Nigeria. From the research, it was concluded that the internal control can be used as an effective tool for fraud control in deposit money banks in Nigeria, James & Lucia (2021)

Risk Assessment of Internal Control and Fraud Prevention of Deposit Money Banks in Nigeria.

The issue and frequent occurrence of fraudulent activities have led to many losses in financial institutions, among which loss of reputation and loss of public confidence are included. Haladu, (2018), studied fraud detection and internal control measures in deposit money banks. It was concluded in the study that the deposit money banks had invested so much in internal control systems that they had not helped reduce fraud in the institution. The study also showed that the internal control measures put in place on the control environment and risk assessment hinder fraud detection and prevention in the institutions. The study concluded that the internal control systems of deposit money banks in Nigeria were inefficient and ineffective.

Information and Communication of Internal Control System and Fraud Prevention of Deposit Money Banks in Nigeria

Fraud is a criminal and carefully planned deceit of the users of the information for the eventual gain of the producer (Ifarajimi, 2022). Information and communication are systems or processes that support the identification, capture, and exchange of information in a form and period that enables people to carry out their responsibilities (Ifarajimi, 2022). A research work conducted by Nyakarimi et al. (2020) investigated the application of the internal control system on fraud prevention in the banking sector. The objective was to establish the effect of the internal control system on fraud prevention in the banking sector. Test results showed control environment of internal control had no significant effect on fraud prevention in the banking sector, the study's hypothesis test revealed information and communication of the internal control system had a significant effect on the prevention of fraud, the result showed that the control mechanisms the organization put in place about communication of information were working appropriately and has a significant effect on fraud prevention (Nyakarimi et al., 2020). Therefore, it was concluded that the mechanisms put in place were not capable of preventing the occurrence of fraud; the parameters were not strong enough based on the findings to address issues of fraud prevention completely from deposit money Banks.

Conceptual framework

The conceptual framework for the present study is depicted in Figure. 2.1 below

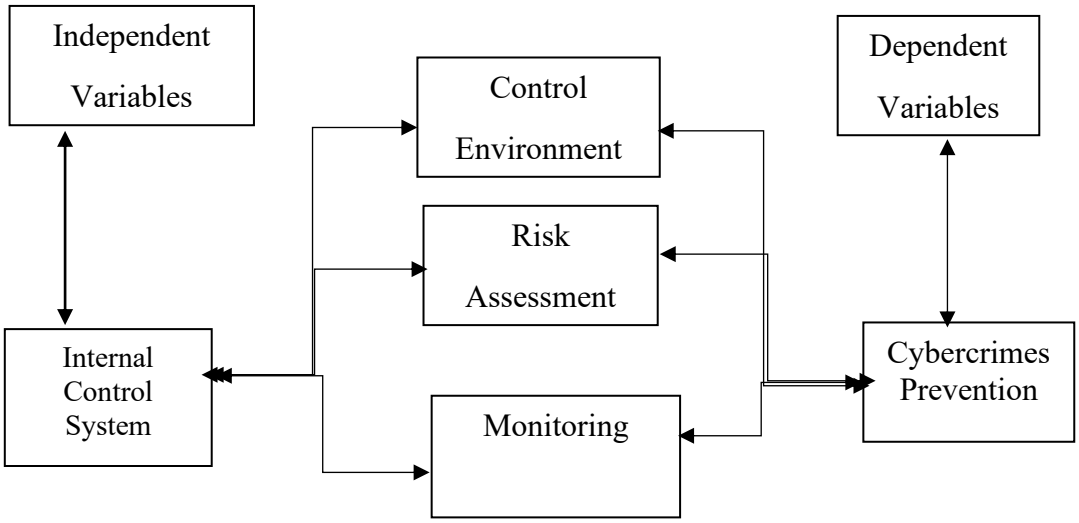


Figure 2.1: Internal Control System vis-à-vis Cybercrimes Prevention

Methodology

This section outlines the methodological framework adopted to investigate how internal control systems influence the prevention of cybercrimes in deposit money banks in Nigeria. It covers the research design, population, sampling techniques, data collection instruments, procedures, and methods of data analysis.

Research Design

The study employed a descriptive survey research design. This design was considered appropriate because it enables the collection of primary data from a cross-section of respondents in their natural settings, allowing for an in-depth assessment of their perceptions and experiences regarding internal control measures and cybercrime prevention in Nigerian deposit money banks.

Population of the Study

The target population will consist of employees of selected deposit money banks operating in Nigeria. Specifically, the focus was on internal control officers, IT security personnel, compliance officers, auditors, and senior operations staff who are knowledgeable about internal controls and cybercrime incidents. The estimated population across the selected banks was 500 employees. While a sample size of 150 respondents was determined using Taro Yamane's formula for finite populations:

n = \frac{N}{1 + N(e)^2}

Where:

n = Sample size

N = Population size (500)

e = Level of precision (0.05)

$$n = \frac{150}{1+500(0.05)^2} = 138$$

However, due to time and resource constraints, a purposive adjustment was made to 120 respondents, which still ensured adequate representation. The study adopted a stratified random sampling technique, stratifying respondents into operational units (Internal Control, IT Security, Audit, and Operations), followed by simple random selection within each stratum.

Sources of Data

The study will make use of both primary and secondary data to underpin the study, as primary Data were collected through structured questionnaires distributed to selected respondents. While the secondary data were obtained from bank policy manuals, annual reports, CBN publications, EFCC reports on cybercrime, and relevant academic literature.

Research Instrument

The instrument used for the primary data collection was a structured questionnaire, segmented into three sections: Section A: Demographic information of respondents. Section B: Questions on the effectiveness of internal control systems (control environment, risk assessment, control activities, information and communication, and monitoring) and Section C: Questions on the incidence and prevention of cybercrimes. The questionnaire used a 5-point Likert scale, ranging from 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree.

Validity and Reliability of the Instrument

To ensure content validity, the questionnaire was reviewed by experts in internal auditing, information security, and academic supervisors. A pilot study was conducted with 15 respondents in one of the deposit money banks to test the reliability. The instrument's internal consistency was assessed using Cronbach's Alpha, yielding a coefficient of 0.83, indicating high reliability.

Method of Data Collection

Questionnaires were personally administered to respondents within their offices to maximize response rates and provide clarification where necessary. Respondents were given two weeks to complete and return the questionnaires.

Method of Data Analysis

Data collected were coded and analysed using the Statistical Package for Social Sciences (SPSS) version 25. Descriptive statistics (mean, frequency, percentages) will be used to summarize responses. Inferential statistics, such as Pearson correlation and regression analysis, will be employed to test the hypotheses and examine the relationship between internal controls and cybercrime prevention effectiveness.

Discussions of Results

This section presents the data collected from respondents, analyses the findings, and interprets the results in line with the study's objectives. The primary goal is to evaluate how internal control systems influence cybercrime prevention in Nigerian deposit money banks. Data was gathered through structured questionnaires distributed to staff members across selected banks. The analysis includes descriptive statistics, inferential statistics using correlation and regression analysis, and a discussion based on the research questions and hypotheses.

Table 1 Response Rate

Out of 150 questionnaires distributed, 138 were completed and returned, representing a **92% response rate**. This high response rate enhances the validity and reliability of the study.

Distributed	Returned	Response Rate
150	138	92%

Table 2 Demographic Information of Respondents

Variable	Frequency	Percentage (%)
Gender		
Male	82	59.4
Female	56	40.6
Age		
18–30	34	24.6

Variable	Frequency	Percentage (%)
31–40	64	46.4
41–50	28	20.3
51 and above	12	8.7
Educational Level		
OND/NCE	18	13.0
HND/B.Sc.	86	62.3
M.Sc./MBA	34	24.7

Analysis of Internal Control Systems in Deposit Money Banks

Respondents were asked to evaluate the effectiveness of internal control systems in their banks using a 5-point Likert scale:

Strongly Agree (5), Agree (4), Neutral (3), Disagree (2), Strongly Disagree (1).

Table 3 Control Environment

Statement	Mean	Std. Dev.
The bank has a strong ethical culture	4.2	0.78
Management enforces compliance with cyber risk policies	4.0	0.85

Table 4 Risk Assessment

Statement	Mean	Std. Dev.
Risk assessments include cyber threats	4.1	0.82
Employees are aware of cybersecurity risks	3.9	0.90

Table 5 Control Activities

Statement	Mean	Std. Dev.
Internal controls are updated regularly	3.8	0.88
Dual control is implemented in sensitive operations	4.0	0.83

Table 6 Information and Communication

Statement	Mean	Std. Dev.
Staff are informed of cyber control procedures	4.1	0.79
Communication systems support internal control goals	4.0	0.86

Table 7 Monitoring Activities

Statement	Mean	Std. Dev.
The bank has an independent audit function	4.2	0.74
Cyber risks are reviewed regularly	3.9	0.91

Table 8 Analysis of Cybercrime Prevention Practices

Statement	Mean	Std. Dev.
Cyber incidents are reported promptly	4.0	0.80
There are clear procedures for responding to cyberattacks	3.8	0.86
Security systems are regularly tested and updated	4.1	0.77
The bank collaborates with authorities on cybercrime prevention	3.9	0.82

Inferential Statistics

Table 9 Correlation Analysis

The Pearson correlation coefficient was used to test the relationship between internal control systems and cybercrime prevention.

Variables	Cybercrime Prevention
Control Environment	0.63**
Risk Assessment	0.58**
Control Activities	0.61**
Information & Communication	0.59**
Monitoring Activities	0.65**

Note: $p < 0.01$ (Significant at 1% level)

This shows a strong positive relationship between internal control components and cybercrime prevention effectiveness.

Table 10 Regression Analysis

To assess the predictive impact of internal control systems on cybercrime prevention:

Regression Model Summary:

Model	R	R^2	Adjusted R^2	Std. Error
1 (All Factors)	0.712	0.507	0.495	0.421

Table 11 ANOVA Table:

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	36.8	5	7.36	41.5	.000
Residual	35.7	132	0.27		
Total	72.5	137			

This model explains approximately 50.7% of the variance in cybercrime prevention practices, suggesting internal controls significantly impact cybercrime mitigation.

Discussion of Findings

This section discusses the major findings of the study on the impact of internal control systems on cybercrime prevention in Deposit Money Banks (DMBs) in Nigeria. The discussion is

organized in line with the study objectives and hypotheses. The analysis confirms a significant relationship between internal control systems and cybercrime prevention efforts. Specifically. The control environment and monitoring activities have the highest correlations with cybercrime prevention, indicating that ethical culture, regular audits, and compliance reviews are key deterrents. While Risk assessment and communication systems also contribute meaningfully, supporting a proactive stance in identifying cyber threats. Banks with stronger internal control frameworks report higher levels of cyber preparedness, response capabilities, and collaboration with authorities. These findings support the study's hypotheses and align with global research that underscores the importance of a robust internal control environment in reducing cybercrime incidents in financial institutions.

1. **Control Environment and Cybercrime Prevention:** The study revealed that the control environment has a significant positive effect on cybercrime prevention in Deposit Money Banks in Nigeria. The result led to the rejection of Hypothesis One (H_{01}). The findings indicate that banks with strong ethical culture, effective corporate governance, management commitment to security, clear policies, and well-defined responsibilities experience lower exposure to cyber fraud. This result suggests that management's attitude toward cybersecurity strongly influences staff behavior. Strong tone-at-the-top discourages insider abuse and system manipulation. Clearly defined roles reduce unauthorized system access. Ethical culture enhances compliance with IT security policies. The implication is that cybercrime prevention begins with leadership commitment and organizational culture. Where management demonstrates seriousness toward internal control and cybersecurity, employees become more cautious and accountable in handling digital transactions. This finding aligns with the theoretical view that the control environment is the foundation of all other internal control components.
2. **Risk Assessment and Cybercrime Prevention:** The study found that risk assessment significantly influences cybercrime prevention, leading to the rejection of Hypothesis Two (H_{02}). This means that Deposit Money Banks that regularly identify, analyse, and evaluate cyber risks are better prepared to prevent cybercrime incidents. Continuous cyber risk assessment helps banks detect new fraud techniques early. Proactive risk identification reduces vulnerability to emerging threats. Cyber risk evaluation supports the development of stronger security policies. Periodic IT risk reviews enhance preparedness against hackers and fraudsters. The finding shows that cybercrime evolves rapidly; therefore, banks that fail to continuously assess risk remain highly vulnerable.
3. **Control Activities and Cybercrime Prevention:** The analysis showed that control activities have a significant impact on cybercrime prevention, resulting in the rejection of Hypothesis Three (H_{03}). Control activities such as: Segregation of duties, Authorization procedures, Access controls, System authentication. Transaction verification. Encryption and firewalls were found to significantly reduce cybercrime occurrences. This implies that when strong operational controls are embedded in digital banking platforms, opportunities for fraud and unauthorized access are minimized. The finding confirms that cybercrime thrives in environments where: Access controls are weak, Password policies are poor, Duties

are not properly segregated, and System checks are inadequate. Thus, robust control activities remain a key defence mechanism against cyber threats.

4. **Information and Communication Systems and Cybercrime Prevention:** The study established that information and communication systems significantly affect cybercrime prevention, leading to the rejection of Hypothesis Four (H**04**). Effective communication and information systems enhance: Timely reporting of suspicious transactions, Real-time fraud alerts and notifications, Staff awareness of cyber threats, Customer awareness of security practices. The findings suggest that banks that invest in secure IT infrastructure and effective communication channels detect cyber threats faster and respond more efficiently. Poor information flow and weak communication systems often delay fraud detection and increase losses.
5. **Monitoring Activities and Cybercrime Prevention:** The study revealed that monitoring activities significantly influence cybercrime prevention, resulting in the rejection of Hypothesis Five (H_{05}). Continuous monitoring activities such as: Internal audit reviews, System surveillance and log monitoring, Compliance checks, Fraud investigation procedures, and Periodic control evaluations were found to significantly reduce cybercrime incidents. This result indicates that internal control systems must not only be implemented but also continuously monitored and updated. Cybercriminals constantly develop new methods; therefore, monitoring ensures that control weaknesses are detected and corrected promptly.

Conclusion and Recommendation

This study examined the impact of internal control systems on cybercrime prevention in deposit money banks in Nigeria. The objective was to determine the extent to which internal control mechanisms, such as the control environment, risk assessment, control activities, information and communication, and monitoring, contribute to mitigating cybercrime in the banking sector. The study concludes by outlining some key findings as follows:

1. **High Response Rate and Qualified Respondents:** The study achieved a 92% response rate from a well-distributed pool of respondents across various age groups and job positions in selected deposit money banks. The majority of respondents held tertiary-level qualifications and were well-versed in banking operations and cybercrime-related issues.
2. **Strong Internal Control Structures:** Respondents reported that their banks had generally strong internal control systems in place. Components such as ethical culture, regular risk assessments, dual control procedures, and consistent monitoring were widely practiced.
3. **Effective Cybercrime Prevention Measures:** Most banks were found to have functional cybersecurity systems and protocols, including regular system audits, timely reporting of cyber incidents, and collaboration with law enforcement agencies.
4. **Statistically Significant Relationship:** Both correlation and regression analyses confirmed a strong positive and statistically significant relationship between internal

control components and cybercrime prevention. The regression model explained about 51% of the variance in cybercrime prevention efforts.

Based on these findings, the study concludes that internal control systems play a crucial role in the prevention and mitigation of cybercrime in Nigerian deposit money banks. Each component of the internal control system, control environment, risk assessment, control activities, information and communication, and monitoring contributes significantly to strengthening a bank's ability to detect, prevent, and respond to cyber threats.

In light of the findings and conclusions, the following recommendations are made:

1. **Strengthen the Control Environment:** Banks should reinforce ethical standards and organizational culture by continuously training employees on integrity, cyber ethics, and compliance. Senior management should lead by example and enforce accountability.
2. **Enhance Risk Assessment Processes:** Risk assessment must be ongoing and dynamic. Banks should integrate advanced threat intelligence tools and periodically update their risk matrices to reflect emerging cyber threats.
3. **Automate and Update Control Activities:** Routine operations such as authorization, approvals, reconciliations, and access controls should be automated where possible to reduce human error and detect irregularities in real time.
4. **Improve Information and Communication Channels:** Cybersecurity awareness should be ingrained across all staff levels. Banks should implement clear and efficient internal communication mechanisms to ensure that all employees understand and follow cyber control policies.
5. **Strengthen Monitoring and Evaluation Mechanisms:** Internal audit units must remain independent and be empowered to assess not just financial risks but also technological vulnerabilities. Monitoring should include frequent testing of systems, incident reporting, and follow-up procedures.

Contributions to Knowledge

This research contributes to the existing body of knowledge by providing empirical evidence on the role of internal control systems in preventing cybercrime within Nigerian banking institutions. It highlights the importance of aligning operational control mechanisms with cybersecurity objectives and provides a framework that can be adapted by other financial institutions.

Limitations of the Study

While this study provides valuable insights, it is limited by the following:

- The research was restricted to a sample of banks and may not fully represent the entire banking sector in Nigeria.
- The study relied on self-reported data, which may be subject to bias.
- Cybercrime is a dynamic and evolving threat; thus, findings may have a time-sensitive relevance.

References

Abdullah, A. H., & Barzinji, Z. (2022). *Kingdom Licensed under Creative Commons, the effect of forensic accounting on fraud prevention, the moderating role*. Abei, A. Y. (2021). Impact of internal control on fraud detection and prevention in microfinance institutions. *Karistad Business School*, *2*(1), 1–68.

Abiola, I. (2021). Internal Control System on Fraud Detection : Nigeria Experience Ladoke Akintola University of Technology Ladoke Akintola University of Technology. *Journal of Accounting and Finance*, *13*(5), 137–149.

Adeleke, O. K., Segun, I. B., & Olaoye, A. C. (2019). Impact of Internal Control on Fraud Prevention in Private Sector Entities in Nigeria. *Journal of Global Economics and Business, 3*(8), 43–55.

Cheng, Q., Goh, B. W., & Kim, J. B. (2018). Internal Control and Operational Efficiency. *Contemporary Accounting Research*, *35*(2), 1102–1139. https://doi.org/10.1111/1911-3846.12409

Chukwuemeka, E., Onah, O. A., & Uzoma, J. (2025). *Smart Contracts and Operational Efficiency of Deposit*. *13*(2), 72–91.

Fabiyi, Aregbesola, Wright, & & O. (2025). Internal Control System and Fraud Prevention in Nigerian Deposit Money Banks. *International Journal of Economics and Financial Issues*, *15*(3), 179–183. https://doi.org/10.32479/ijefi.17537

Fijabi, L. K., Owolabi, S. A., & Ajibade. (2022). A Comparative Study of Financial Management Practices on the Performance of Quoted Manufacturing and Oil and Gas Firms in Nigeria. *Caleb International Journal of Development Studies*, *05*(01), 70–95. https://doi.org/10.26772/cijds-2022-05-01-05

Haladu, A. (2018). *Fraud Detection and Internal Control Measures in Deposit Money Banks Listed on the NSE*. *December*, 43–54.

Hudu, A. S. (2020). Internal Control system and fraud. *Journal of Accounting and Financial Studies*, *8172*(1), 1–65.

Ifarajimi, G. @ A. S. (2022). *Internal Control and Financial Fraud in The Nigerian Banking Industry*. *5*(1).

James, I., & Lucia, U. (2021). Internal Control: A Tool for Fraud Control in Deposit Money Banks in Nigeria. *European Journal of Business and Management*, *13*(13), 64–75. https://doi.org/10.7176/ejbm/13-13-07

Kizil, C., Kizil, F., & Dolaz, B. (2021). Reconsidering the role of internal controls in the COVID-19 era. *The Institute for Internal Controls (IIC) e-Magazine*, *2*(2), 9–19.

Munira, H., Hazmi, Y., Ramadhani, Z. D., & Syahira, C. Y. (2024). Internal Control System. In *The ES Accounting and Finance* (Vol. 2, Issue 03, pp. 166–171). https://doi.org/10.58812/esaf.v2i03.295

Ngigi Nyakarimi, S., Nduati Kariuki, S., & Ombe Kariuki, P. W. (2020). Risk Assessment and Fraud Prevention in the Banking Sector. *The Journal of Social Sciences Research*, *6*(61), 13–20. https://doi.org/10.32861/jssr.61.13.20

Rae, K., & Sands. (2017). Associations among the Five Components within COSO Internal Control-Integrated Framework as the Underpinning of Quality Corporate Governance. *Australasian Accounting, Business and Finance Journal*, *11*(1), 28–54. https://doi.org/10.14453/aabfj.v11i1.4

Samuel, O. A., Pelumi, I. O., & Fasilat, O. O. (2021). Effect of internal control system on fraud prevention among deposit money banks in Kwara State, Nigeria. *International Journal of Multidisciplinary Research and Growth Evaluation*, *2*(1), 264–271. https://www.allmultidisciplinaryjournal.com/archivesarticle/2021.v2.i1.118.pdf

Shehu, T. S. (2025). Internal Control System and Fraud Mitigation: A Case of Selected SMEs in Nigeria. *Asian Journal of Advanced Research and Reports*, *19*(4), 301–315. https://doi.org/10.9734/ajarr/2025/v19i4985

Tenbele, N. T. (2019). Effectiveness of the internal control system in higher learning institutions in Nairobi, Kenya. *Global Journal of Business, Economics and Management: Current Issues*, *9*(3), 143–155. https://doi.org/10.18844/gjbem.v9i3.4399

Vutumu, A., Aregbeyen, O., & Akinteye, A. S. (2024). Internal Control and Fraud Prevention in the Nigerian Public Sector: A Partial Least Squares Structural Equation Modeling Approach. *Journal of Financial Risk Management*, *13*(04), 703–729. https://doi.org/10.4236/jfrm.2024.134034

Wanjala, K., & Riitho, D. (2020). Internal Control Systems Implementation and Fraud Mitigation Nexus among Deposit Taking Saccos in Kenya. *Finance & Economics Review*, *2*(1), 11–29. https://doi.org/10.38157/finance-economics-review.v2i1.59

Yusuf, M., & Kanji, L. (2020). Effect of Internal Audit and Accounting Information System on the Effectiveness of Internal Control. *Atestasi : Jurnal Ilmiah Akuntansi*, *3*(2), 120–125. https://doi.org/10.57178/atestasi.v3i2.222

Zira, R. A., & Suleiman, A. (2024). The Impact of Cyber-Crimes on Depositors Accounts in Some Selected Deposit Money Banks in Bauchi State, Nigeria. *IIARD International Journal of Banking and Finance Research E-IIARD International Journal of Banking and Finance Research E*, *10*(10), 200–211. https://doi.org/10.56201/ijbfr.v10.no10.2024.pg200.211