VOL. 13 NO. 7,
AUGUST, 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)

Forensic Accounting Practices and Cybercrime Control in Nigerian Deposit Money Banks

Adeleke, Adebowale Babawale; & Adedipe Oluwaseyi Ayodele (PhD)

Department of Accounting and Finance, Faculty of Management Sciences, Ajayi Crowther University, Oyo,
Corresponding Author: ab.adeleke@acu.edu.ng
DOI: https://doi.org/10.70382/ajbdmr.v13i7.092

Abstract

This study examines the effect of forensic accounting practices and regulatory compliance investigations on cybercrime control in selected Nigerian deposit money banks. A survey research design was adopted, and primary data were collected from 142 top management staff across 13 listed banks in Lagos State, Nigeria. Structured questionnaires were used for data collection, while data were analyzed using descriptive statistics and ordinary least squares (OLS) regression analysis. The findings reveal that forensic accounting software ($\beta = 0.295$, $p = 0.012$) and data mining tools ($\beta = 0.323$, $p = 0.001$) have significant positive effects on cybercrime control. Evidence from Central Bank of Nigeria (CBN), Economic and Financial Crimes Commission (EFCC), and Nigeria Deposit Insurance Corporation (NDIC) reports confirms persistent cybercrime incidents despite regulatory frameworks, supporting the empirical findings. The study concludes that forensic accounting technologies play a more significant role in cybercrime control than traditional audit and compliance mechanisms in Nigerian deposit money banks. It recommends increased investment in forensic technologies, enhanced regulatory enforcement, and stronger integration of compliance systems with digital fraud detection tools.

Keywords: Forensic Accounting Practices, Cybercrime Control, Data mining, Regulatory Compliance, Audit review reports.

Introduction

According to the Central Bank of Nigeria (CBN) and the Nigeria banking regulatory framework, the banking industry in Nigeria plays a fundamental role in economic development by mobilising savings, facilitating credit creation, and supporting both domestic and international

financial transactions. Deposit money banks (DMBs) serve as the core of this financial system by providing digital and non-digital financial services that drive economic activities. With the rapid expansion of electronic banking channels such as internet banking, mobile banking, and electronic payment systems, the Nigerian banking sector has become highly technology-driven. However, scholars have observed that this digital transformation has also increased exposure to cyber threats and financial fraud. Olabisi S.O. (2024) explained that the growing sophistication of cybercrime in Nigerian banks makes traditional control mechanisms insufficient. Similarly, Ole (2023) argued that digital banking expansion has created new vulnerabilities that require advanced technological and forensic responses. In response, cybercrime control practices such as cybersecurity frameworks, regulatory monitoring, and internal control systems have become essential tools for safeguarding banking operations.

Furthermore, forensic accounting practices have been widely acknowledged as a critical component of cybercrime control in the banking sector. According to Enofe et al. (2015), forensic accounting involves the use of investigative accounting techniques to detect and prevent financial irregularities in organisations. Ogunleye & Fanimokun (2025) explained that data mining tools and forensic software enable banks to analyse large volumes of financial data and identify suspicious transaction patterns in real time. Similarly, Onourah and Appah (2022) observed that forensic accounting practices significantly improve fraud detection and strengthen internal control systems in financial institutions. Gbegi and Adebisi (2024) also argued that forensic accounting techniques enhance transparency and accountability in banking operations, although their effectiveness depends on proper implementation and institutional support. Owolabi et al. (2023) further noted that digital forensic tools improve cybercrime detection but may be limited by inadequate technical skills and weak system integration. Despite these improvements, CBN and EFCC reports continue to show persistent cases of cyber fraud in Nigerian deposit money banks, indicating that cybercrime control remains a major concern in the sector.

Statement of the Problem

Despite the increasing adoption of forensic accounting software, data mining tools, audit review systems, and regulatory compliance frameworks, cybercrime continues to persist in Nigerian deposit money banks. According to Olabisi S.O. (2024), forensic accounting software significantly improves fraud detection; however, cybercrime incidents are still frequently reported, suggesting that technological adoption alone is not sufficient. Ole (2023) also observed that although digital analytics tools enhance monitoring and fraud prevention, they do not completely eliminate cyber risks in banking operations. Similarly, Ogunleye & Fanimokun (2025) argued that while data mining tools improve transaction monitoring and fraud detection, their effectiveness is limited by challenges such as inadequate technical expertise and poor system integration. These studies collectively indicate that there is still a gap between the deployment of forensic technologies and actual cybercrime control effectiveness.

In addition, studies have shown that regulatory compliance and audit-based mechanisms are not yielding optimal outcomes in cybercrime control. Onourah and Appah (2022) explained that although forensic accounting and audit systems contribute to fraud detection, their effectiveness depends largely on implementation quality and organisational commitment. Gbegi and Adebisi (2024) observed that audit and forensic techniques improve fraud detection only when properly enforced, while weak institutional support reduces their impact. Owolabi et al. (2023) further argued that the effectiveness of cybercrime control systems is constrained by inadequate technical capacity and weak organisational integration of forensic tools. Furthermore, EFCC and CBN reports have consistently highlighted

increasing cases of cyber fraud in Nigerian banks despite regulatory reforms. These conditions suggest that cybercrime control in Nigerian deposit money banks remains inadequate, creating a clear problem of whether forensic accounting practices and regulatory compliance investigations are truly effective in controlling cybercrime. It is against this background that this study seeks to empirically examine their relationship.

Research Questions

1. To what extent do Forensic accounting software influence cybercrime detection and prevention in Nigerian deposit money banks?
2. What is the relationship between data mining tools and technology on cybercrime control in Nigeria deposit money banks?

Objectives of the Study

This study generally examines the effect of forensic accounting practices on cybercrime control in selected Nigerian deposit money banks. Other specific objectives are to:

i. ascertain the effect of forensic accounting software on cybercrime in selected Nigerian deposit money banks
ii. examine the relationship between data mining tools and technology on cybercrime control in selected Nigeria deposit money banks

Forensic Accounting Practices in Nigerian Deposit Money Banks

Forensic accounting practices involve the use of accounting, auditing, and investigative techniques to detect and prevent fraud and cyber-related financial crimes in banks. In Nigerian deposit money banks, these practices are increasingly important due to rising cases of electronic fraud and financial manipulation. Studies by Enofe, Omagbon and Ehigiator (2025) and Dada et al. (2023) show that forensic accounting improves fraud detection and strengthens internal control systems. Similarly, Okoye and Gbegi (2023) note that it helps banks identify irregular financial activities and reduce opportunities for cybercrime. Regulatory bodies such as the CBN and EFCC also encourage stronger forensic systems to improve financial transparency and accountability.

Forensic Accounting Software

Forensic accounting software refers to digital tools used to detect fraud, analyze financial data, and monitor suspicious transactions in real time. These tools improve the speed and accuracy of fraud detection in banks. Bierstaker, Brody and Pacini (2024) explain that such software enhances auditors' ability to identify unusual financial patterns. Singleton and Singleton (2020) also highlight that it supports efficient fraud investigation through data visualization and analysis. In Nigeria, Olabisi (2024) and Ogunleye & Fanimokun (2025) found that forensic software significantly improves cybercrime detection in banks, although its effectiveness depends on proper usage and staff competence.

Data Mining Tools and Technology

Data mining tools and technology are used to analyze large volumes of financial data to detect patterns, anomalies, and suspicious transactions. In banks, they are important for early fraud detection and cybercrime prevention. Hand, Mannila and Smyth (2001) describe data mining as a key tool for extracting useful information from large datasets. In Nigeria, Akinyemi and Adegbie (2022) and Oladimeji and Adegbie (2023) found that data mining improves fraud detection and monitoring systems

in financial institutions. However, Owolabi et al. (2013) argue that its effectiveness depends on skilled personnel and proper system integration.

Cybercrime Control in Nigerian Banking Sector

Cybercrime control refers to the strategies used by banks to prevent, detect, and respond to cyber-related financial crimes such as hacking and online fraud. In Nigeria, cybercrime has become a serious challenge due to increased digital banking activities. According to CBN (2023) and EFCC (2024), cyber fraud cases continue to rise in the banking sector. Choo (2011) explains that effective cybercrime control requires a combination of technology, regulation, and human expertise. Similarly, Amedu and Nwankwo (2022) stress the need for stronger digital security systems and forensic tools. However, Adeyemi and Adebayo (2023) note that weak enforcement and limited infrastructure still hinder effective cybercrime control in Nigerian banks.

Technology Theory

Technology Theory in this study is grounded in the works of Rogers (1962), who propounded the Diffusion of Innovations Theory, and Davis (1989), who developed the Technology Acceptance Model (TAM). Rogers (1962) assumes that the adoption of new technology in organizations depends on its relative advantage, compatibility, complexity, trialability, and observability, while Davis (1989) assumes that perceived usefulness and perceived ease of use determine the acceptance and effective utilization of technology. The theory further assumes that organizations that adopt relevant technologies will experience improved efficiency, effectiveness, and decision-making outcomes. Critics of Technology Theory argue that it is overly deterministic and tends to underplay institutional, behavioural, and environmental constraints that may hinder effective technology adoption, even when systems are available (Bagozzi, 2007; Legris, Ingham & Collerette, 2003). It has also been criticized for assuming rational decision-making processes that may not fully reflect real organizational behaviour in developing economies. In relation to this study, Technology Theory is highly relevant because forensic accounting software and data mining tools in Nigerian deposit money banks function as technological innovations that improve cybercrime detection, enhance transaction monitoring, and strengthen internal control systems. Empirical studies by Olabisi (2024) and Ogunleye & Fanimokun (2025) support this position by showing that technological forensic tools significantly improve fraud detection and cybercrime control in Nigerian banks.

Fraud Diamond Theory

The Fraud Diamond Theory was propounded by Wolfe and Hermanson (2004) as an extension of Cressey's (1953) Fraud Triangle Theory. While Cressey (1953) identified pressure, opportunity, and rationalization as key drivers of fraud, Wolfe and Hermanson (2004) added "capability" as a fourth dimension, arguing that fraud can only occur if the individual has the necessary skills, position, and ability to exploit system weaknesses. The theory assumes that fraud prevention can be achieved by reducing opportunity through strong internal controls, monitoring systems, and technological safeguards. Critics of the theory argue that it overemphasizes individual traits and behavioural factors while underestimating broader systemic, organisational, and technological influences on fraud occurrence (Dorminey et al., 2012; Hogan, Rezaee, Riley & Velury, 2008). It is also criticised for being more descriptive than predictive in complex organisational environments. In this study, the Fraud Diamond Theory is relevant because forensic accounting practices, data mining tools, and cyber monitoring systems in Nigerian deposit money banks directly reduce the "opportunity" element of fraud

by increasing surveillance, improving anomaly detection, and limiting access to vulnerable systems. Studies such as Onuorah and Appah (2012) and Dada et al. (2023) support the application of this theory by showing that strengthened forensic and control systems significantly reduce fraudulent activities in financial institutions.

Inspired Confidence Theory

The Inspired Confidence Theory was propounded by Limperg in 1932. The theory assumes that the primary objective of auditing and assurance services is to inspire confidence among stakeholders by ensuring that financial statements and organizational systems are reliable and trustworthy. It further assumes that auditors derive their mandate from societal expectations and must perform their duties in a manner that sustains public confidence in financial reporting systems (Limperg, 1932). Critics of the theory argue that it is conceptually abstract, lacks precise operationalization, and is difficult to measure empirically in practical research settings (Flint, 1988; Porter, 1993). It is also criticized for placing excessive responsibility on auditors without adequately considering structural and technological constraints within organizations. Despite these limitations, the theory remains relevant to this study as it explains how forensic accounting practices, data mining tools, and regulatory compliance mechanisms enhance stakeholder confidence in Nigerian deposit money banks. By improving fraud detection, strengthening audit review systems, and ensuring regulatory adherence, these mechanisms inspire trust among customers, regulators, and investors. Empirical support is provided by studies such as Enofe et al. (2015) and Okoye and Gbegi (2013), which show that forensic accounting and audit mechanisms improve transparency and reduce fraudulent activities in financial institutions.

Empirical Studies

Onourah and Appah (2022) studied the role of forensic accounting in fraud detection and prevention in financial institutions in Nigeria. The study adopted a cross-sectional survey research design and focused on selected banks and financial institutions. The population consisted of accounting and audit personnel, with a sample size of about 160 respondents selected using simple random sampling technique. Data were collected through structured questionnaires. The study used descriptive statistics and regression analysis for data analysis. The findings revealed that forensic accounting practices significantly enhance fraud detection and internal control effectiveness. The study concluded that forensic accounting is an essential tool for reducing financial irregularities in the banking sector.

Owolabi et al. (2023) investigated the relationship between digital forensic tools and fraud control in Nigerian financial institutions. The study used a descriptive survey research design and focused on selected deposit money banks. The population included audit and compliance staff, with a sample size of approximately 190 respondents selected through stratified sampling. Data were collected using structured questionnaires and analyzed using correlation and regression analysis. The findings showed that digital forensic tools positively influence fraud detection and cybercrime control, but their effectiveness is limited by inadequate technical skills and poor system integration. The study concluded that forensic technologies improve fraud control but require proper implementation and skilled personnel.

Ole (2023) examined the effect of data analytics and digital tools on fraud prevention in Nigerian banks. The study adopted a survey research design and focused on selected deposit money banks in Nigeria. The population consisted of banking professionals in audit, ICT, and risk management units, with a sample size of 170 respondents selected using stratified random sampling. Data were collected through structured questionnaires. The study employed descriptive statistics and regression analysis to test

hypotheses. The findings revealed that digital analytics tools significantly improve fraud detection and cybercrime monitoring. The study concluded that advanced data analytics systems are essential for strengthening fraud prevention mechanisms in Nigerian banking institutions.

Gbegi and Adebisi (2024) examined the effectiveness of forensic accounting techniques in fraud prevention and detection in Nigerian public and private sector organizations, including banks. The study adopted a survey research design with a population drawn from accounting professionals and auditors. A sample size of 220 respondents was selected using stratified sampling technique. Data were collected using structured questionnaires and analyzed using regression and descriptive statistics. The findings indicated that forensic accounting techniques significantly influence fraud detection when properly implemented. However, the study also noted that weak institutional support and poor implementation reduce effectiveness. The study concluded that forensic accounting is effective but requires strong organizational commitment and training.

Olabisi (2024) examined the effect of forensic accounting software on fraud detection and cybercrime control in Nigerian deposit money banks. The study adopted a descriptive survey research design and focused on selected commercial banks in Nigeria. The population comprised staff involved in audit, compliance, and ICT-related functions, with a sample size of 200 respondents selected using stratified random sampling technique. Data were collected primarily through structured questionnaires. The study employed descriptive statistics and multiple regression analysis to test the hypotheses. The findings revealed that forensic accounting software has a significant positive effect on fraud detection and cybercrime control. The study concluded that the adoption of forensic accounting software enhances real-time fraud monitoring and strengthens internal control systems in Nigerian banks.

Ogunleye and Fanimokun (2025) investigated the impact of data mining tools on fraud prevention and financial reporting quality in Nigerian deposit money banks. The study adopted a survey research design and covered selected banks in Lagos and Abuja. The population included employees from audit, risk management, and ICT departments, with a sample size of 180 respondents selected using purposive and stratified sampling techniques. Data were collected using structured questionnaires and supported with secondary data from annual reports. The study employed correlation and regression analysis for data evaluation. The findings showed that data mining tools significantly improve fraud detection, transaction monitoring, and financial reporting accuracy. The study concluded that data analytics technologies play a vital role in strengthening cybercrime control and improving banking efficiency.

Methodology

This study adopted a survey research design to examine the effect of forensic accounting practices and regulatory compliance investigations on cybercrime control in selected Nigerian deposit money banks. The survey design was considered appropriate because it enables the collection of primary data from respondents and allows for the statistical analysis of relationships among variables in a real organisational setting. The target population comprised all top management staff at the headquarters of thirteen (13) listed deposit money banks in Lagos State, Nigeria. According to the field survey and institutional records, the population consists of 204 top management staff across the selected banks, as presented in Table 3.1 below. These respondents are considered suitable because they are directly involved in audit, risk management, compliance, and cybersecurity-related decision-making within their respective institutions.

Table 1: The target population of the firms with the number of top management staffs

S/N	SECTOR	Staffs
1	Access Bank Plc.	13
2	Zenith Bank Plc	15
3	Wema Bank Plc	13
4	Unity Bank Plc	9
5	UBA	16
6	Stanbic IBTC	14
7	Sterling Financial Holdings	9
8	Jaiz Bank	15
9	Guarantee Trust Bank	31
10	Fidelity Bank	30
11	FCMB	15
12	First Bank of Nigeria	9
13	Ecobank	15
	Total	**204**

Source: Researcher's Compilation, 2025

The Taro Yamane formula (1967) of sample size will be applied to obtain the representative sample size for the study. The following formula applies:

$$\mathbf{n} = \frac{N}{1+N\,(e^{e})}$$

Where;

n = sample size

N = population

1 = constant

e = level of significant to be set at 5 percent or 0.05

Sample size calculation

$$n = \frac{204}{1 + 204\,(005^2)}$$

$$n = \frac{204}{1.51}$$

$$n = 135.10$$

$$n = 135$$

To account for possible non-response and incomplete questionnaires, a 5% adjustment was added, bringing the final sample size to 142 respondents. The study relied primarily on primary data collected through structured questionnaires administered to selected respondents in the participating banks. The questionnaire was designed using a five-point Likert scale to capture responses on forensic accounting practices, regulatory compliance investigations, and cybercrime control. Cronbach's Alpha was used to test the reliability and internal consistency of the measurement instruments, while content and construct

validity were ensured through expert review and alignment with existing literature. Data collected were analyzed using descriptive and inferential statistical techniques. Descriptive statistics such as frequency distribution, percentages, mean, and standard deviation were used to summarize respondents' characteristics and responses. The results were presented using tables and charts for clarity and ease of interpretation.

Table 2: Distribution of Questionnaire by States

Questionnaires	Responses	Percentage (%)
Number of filled	133	93.66
Number Not Returned	9	6.34
Total	142	100%

Source: Field Survey, (2026)

Table 4.1 presents the distribution and return rate of questionnaires administered to respondents in selected Nigerian deposit money banks. A total of 142 questionnaires were distributed to the target respondents, out of which 133 were properly completed and returned, representing a high response rate of 93.66%. However, 9 questionnaires were not returned, accounting for 6.34% of the total administered. The high response rate indicates strong participation from the respondents and suggests that the data collected is reliable and adequate for further statistical analysis.

Table 3: Bio-data of the Respondents

		Frequency	Percent
Gender	Male	106	79.7
	Female	27	20.3
Position in Bank	Internal Auditor	77	57.9
	Forensic Accountant	16	12.0
	Compliance Officer	20	15.0
	IT/Cybersecurity Officer	10	7.5
	Branch Manager	10	7.5
Years of Working Experience	1-5 years	49	36.8
	6-10 years	52	39.1
	11-15 years	24	18.0
	Above 15 years	8	6.0
Bank Category	Large Banks	98	73.7
	Medium Banks	35	26.3

Source: Data Output, 2026.

Table 4.2 presents the bio-data of the 133 respondents drawn from selected Nigerian deposit money banks, offering detailed insight into their demographic and professional characteristics relevant to this study. The gender distribution reveals that 106 respondents, representing 79.7%, are male, while 27 respondents, accounting for 20.3%, are female. This indicates a clear predominance of male respondents within the selected banking roles. The disparity suggests that the workforce in areas related to forensic accounting, compliance, and cybercrime control is largely male-dominated, which is reflective of the broader structure within many financial institutions in Nigeria.

With respect to respondents' positions within the banks, the data show that a significant proportion, 77 respondents (57.9%), are Internal Auditors. This is followed by Compliance Officers who constitute 20 respondents (15.0%), and Forensic Accountants with 16 respondents (12.0%). IT/Cybersecurity Officers and Branch Managers each account for 10 respondents (7.5%) respectively. This distribution indicates that the majority of participants are directly involved in audit and control functions, which are central to fraud detection, regulatory compliance, and financial monitoring processes within banks. The presence of respondents across multiple professional roles ensures that the study captures diverse but relevant perspectives on cybercrime control mechanisms.

In terms of years of working experience, the findings indicate that 52 respondents (39.1%) have between 6–10 years of experience, while 49 respondents (36.8%) have between 1–5 years of experience. Additionally, 24 respondents (18.0%) fall within the 11–15 years category, and only 8 respondents (6.0%) have more than 15 years of experience. This distribution shows that the majority of respondents are within the early to mid-career stages, suggesting that they are actively engaged in current banking practices and evolving technological and regulatory frameworks. The relatively smaller proportion of highly experienced respondents indicates limited representation from long-tenured professionals.

Furthermore, the classification of banks indicates that a larger proportion of respondents, 98 (73.7%), are drawn from large banks, while 35 respondents (26.3%) are from medium-sized banks. This suggests that the data is more reflective of practices within large banking institutions, which typically have more structured systems, advanced technological infrastructure, and stronger regulatory frameworks. The inclusion of respondents from both large and medium banks, however, provides some level of variation in institutional perspectives. Overall, the bio-data demonstrates that the respondents are predominantly professionals in audit, compliance, and financial control roles, with considerable representation from large banks and individuals possessing moderate levels of work experience. This provides a relevant and credible basis for analyzing the effect of forensic accounting practices and regulatory compliance on cybercrime control in Nigerian deposit money banks.

Descriptive Analysis of Variables Item Responses

The responses from staff of selected Nigerian deposit money banks to the research questions relating to the study variables are presented and analyzed in Tables 4.3, 4.4, 4.5, 4.6, and 4.7 below.

Table 4: Descriptive statistics on responses to Forensic Accounting Software and Cybercrime Control

Items	Responses					Total
	SA	A	U	D	SD	
The use of forensic accounting software enhances early detection of cyber fraud.	66 (49.6%)	45 (33.8%)	-	22 (16.5%)	-	133 (100%)
Forensic audit software improves real-time monitoring of suspicious transactions.	65 (48.9%)	20 (15%)	19 (14.3%)	6 (4.5%)	23 (17.3%)	133 (100%)
Forensic software significantly reduces cybercrime incidents in our bank.	126 (94.7%)	5 (3.8%)	-	2 (1.5%)	-	133 (100%)
The bank regularly updates its forensic accounting software to combat cyber threats.	26 (19.5%)	72 (54.1%)	-	35 (26.4%)	-	133 (100%)

Items	Responses					Total
	SA	A	U	D	SD	
Forensic software improves digital evidence gathering for cybercrime investigations.	59 (44.4%)	39 (29.3%)	-	35 (26.3%)	-	133 (100%)

Source: Data Output, 2026.

The responses in Table 4.3 provide a clear indication of how employees in selected Nigerian deposit money banks perceive the role of forensic accounting software in cybercrime control. Overall, the results show a strong positive view of the software's effectiveness, suggesting that respondents generally believe these tools are essential for combating cyber threats in the banking sector. This reflects the widespread recognition among banking staff that integrating forensic accounting technology is a key part of institutional efforts to safeguard financial systems.

A significant proportion of respondents, 66 (49.6%) strongly agreed and 45 (33.8%) agreed, that forensic accounting software enhances the early detection of cyber fraud, while only 22 (16.5%) disagreed. These findings indicate that most respondents acknowledge the software's role in identifying fraudulent activities promptly, which is critical for reducing potential financial losses and preventing the escalation of cybercrime within banks. The high level of agreement underscores the perceived value of early detection mechanisms supported by advanced forensic tools.

Regarding the capacity for real-time monitoring of suspicious transactions, 65 respondents (48.9%) strongly agreed and 20 (15%) agreed that forensic audit software improves monitoring, while 19 (14.3%) were undecided, 6 (4.5%) disagreed, and 23 (17.3%) strongly disagreed. This shows that although a majority of respondents perceive real-time monitoring as a benefit of forensic software, there is some variability in opinion, likely reflecting differences in software implementation, training, or technical infrastructure across banks. Nevertheless, the overall positive perception highlights the important role of forensic tools in actively tracking and addressing suspicious financial activities.

An overwhelming majority of respondents, 126 (94.7%), strongly agreed that forensic software significantly reduces cybercrime incidents in their banks, with only a minimal proportion expressing disagreement. This demonstrates a strong consensus among banking staff that forensic accounting tools are highly effective in preventing and mitigating cybercrime. The near-unanimous agreement reinforces the perception that such technology is a fundamental component of cybercrime control strategies within the sector. The study also revealed that 26 respondents (19.5%) strongly agreed and 72 (54.1%) agreed that banks regularly update their forensic accounting software to address cyber threats, while 35 (26.4%) disagreed. This indicates that while most respondents believe software updates are implemented consistently, a notable proportion feel that updates may not always be timely or uniform across all institutions. Regular updates are critical for maintaining the effectiveness of these tools, as cybercriminals continually develop new methods to bypass security measures.

Finally, 59 respondents (44.4%) strongly agreed and 39 (29.3%) agreed that forensic accounting software improves digital evidence gathering for cybercrime investigations, whereas 35 (26.3%) disagreed. This suggests that most respondents recognize the software's importance in supporting investigative processes, though some concerns about implementation, accessibility, or technical limitations remain. Overall, the findings indicate that forensic accounting software is widely viewed as essential for enhancing cybercrime detection, monitoring, prevention, and investigation within Nigerian deposit money banks.

Table 5: Descriptive statistics on responses to Data Mining Tools and Technology

Items	Responses					Total
	SA	A	U	D	SD	
Data mining tools help detect unusual transaction patterns.	43 (32.3%)	20 (15%)	25 (18.8%)	30 (22.6%)	15 (11.3%)	133 (100%)
Advanced technology improves fraud detection accuracy in our bank.	63 (47.4%)	21 (15.8%)	13 (9.8%)	28 (21.1%)	8 (6%)	133 (100%)
The use of analytics tools strengthens cybercrime prevention mechanisms.	59 (44.4%)	46 (34.6%)	3 (2.3%)	13 (9.8%)	12 (9%)	133 (100%)
Data mining technology enhances monitoring of electronic banking transactions.	57 (42.9%)	36 (27.1%)	8 (6%)	14 (10.5%)	18 (13.5%)	133 (100%)
Technological tools significantly improve cybercrime control in the bank.	55 (41.4%)	28 (21.1%)	28 (21.1%)	18 (13.5%)	4 (3.0%)	133 (100%)

Source: Data Output, 2026.

Table 4.4 presents the descriptive statistics on respondents' perceptions of the role of data mining tools and technology in enhancing cybercrime control in selected Nigerian deposit money banks. The data reveal that 43 respondents (32.3%) strongly agreed and 20 respondents (15%) agreed that data mining tools help detect unusual transaction patterns, while 30 respondents (22.6%) disagreed and 15 (11.3%) strongly disagreed, indicating that although a significant proportion of staff recognize the importance of data mining for identifying irregularities, there remains a notable level of skepticism or uncertainty about its effectiveness. Similarly, 63 respondents (47.4%) strongly agreed and 21 (15.8%) agreed that advanced technology improves fraud detection accuracy, whereas 28 respondents (21.1%) disagreed and 8 (6%) strongly disagreed, reflecting a generally positive perception of technological enhancements in fraud prevention but highlighting areas where implementation may be inconsistent.

The findings further show that 59 respondents (44.4%) strongly agreed and 46 (34.6%) agreed that the use of analytics tools strengthens cybercrime prevention mechanisms, with only 13 respondents (9.8%) disagreeing and 12 (9%) strongly disagreeing. This suggests that the majority of staff perceive analytics tools as effective in supporting proactive cybercrime control measures. In addition, 57 respondents (42.9%) strongly agreed and 36 (27.1%) agreed that data mining technology enhances the monitoring of electronic banking transactions, while 14 respondents (10.5%) disagreed and 18 (13.5%) strongly disagreed. These responses highlight the perceived value of continuous transaction monitoring as part of technological interventions, though differences in perception may reflect variations in access, system sophistication, or training among banks.

Finally, 55 respondents (41.4%) strongly agreed and 28 (21.1%) agreed that technological tools significantly improve cybercrime control in their banks, whereas 18 respondents (13.5%) disagreed and 4 (3%) strongly disagreed, with 28 respondents (21.1%) remaining undecided. The findings demonstrate that the majority of respondents recognize the critical role of data mining and technological tools in detecting fraud, monitoring transactions, and enhancing cybercrime control. At the same time, the presence of undecided and dissenting responses suggests that while technology is widely

acknowledged as important, factors such as training, software availability, and system updates may influence the consistency of its application across different banks.

Table 6: Descriptive statistics on responses to Cybercrime Control

Items	Responses					Total
	SA	A	U	D	SD	
Cybercrime incidents have reduced in our bank over the past few years.	37 (27.8%)	39 (29.3%)	5 (3.8%)	32 (24.1%)	20 (15%)	133 (100%)
Our bank has strong cyber security protocols.	66 (49.6%)	54 (40.6%)	-	8 (6%)	5 (3.8)	113 (100%)
The bank responds quickly to cyber incidents.	70 (52.6%)	34 (25.6%)	-	19 (14.3%)	10 (7.5%)	133 (100%)
Fraud detection systems are highly effective.	43 (32.3%)	20 (15%)	25 (18.8%)	30 (22.6%)	15 (11.3%)	133 (100%)
Overall, cybercrime control mechanisms in our bank are effective.	59 (44.4%)	46 (34.6%)	3 (2.3%)	13 (9.8%)	12 (9%)	133 (100%)

Source: Data Output, 2026.

Table 4.5 presents the descriptive statistics on respondents' perceptions of cybercrime control in selected Nigerian deposit money banks. The data reveal that while there is a general perception of improvement, responses vary across different measures of cybercrime control. For example, 37 respondents (27.8%) strongly agreed and 39 (29.3%) agreed that cybercrime incidents have reduced in their banks over the past few years, whereas 32 (24.1%) disagreed and 20 (15%) strongly disagreed, with 5 (3.8%) undecided. This indicates that although a majority recognize a decline in cybercrime, a notable proportion of respondents perceive that incidents remain significant, suggesting differences in experience or reporting across institutions.

Respondents also reported positively on the strength of cybersecurity protocols, with 66 (49.6%) strongly agreeing and 54 (40.6%) agreeing that their banks have strong systems, while only 8 (6%) disagreed and 5 (3.8%) strongly disagreed. Similarly, 70 respondents (52.6%) strongly agreed and 34 (25.6%) agreed that banks respond quickly to cyber incidents, although 19 (14.3%) disagreed and 10 (7.5%) strongly disagreed. These findings suggest that robust cybersecurity measures and rapid incident response are widely recognized as important components of cybercrime control within the banking sector.

In contrast, perceptions of fraud detection systems were less uniform. While 43 respondents (32.3%) strongly agreed and 20 (15%) agreed that fraud detection systems are highly effective, 30 (22.6%) disagreed and 15 (11.3%) strongly disagreed, with 25 (18.8%) undecided. This variability indicates that while some banks have effective detection mechanisms, others may face challenges in fully implementing or maintaining these systems. When considering the combined effectiveness of cybercrime control mechanisms, 59 respondents (44.4%) strongly agreed and 46 (34.6%) agreed that their banks' systems are effective, whereas 13 (9.8%) disagreed, 12 (9%) strongly disagreed, and 3 (2.3%) were undecided. This demonstrates that, despite some variability in specific areas such as fraud detection or reduction of incidents, most respondents perceive that the banks' cybercrime control

measures are generally effective. Collectively, the findings indicate that Nigerian deposit money banks have made significant progress in implementing systems and protocols to prevent, detect, and respond to cybercrime, although consistent performance across all banks remains an area for improvement.

Effect of forensic accounting software on cybercrime in selected Nigerian deposit money banks

$CCC_i = \beta_0 + \beta_1 FAS_i + \beta_2 BS_i + \beta_3 TI_i + \beta_4 AGE_i + \varepsilon_i$

Table 7: Ordinary Least Square for Model I

Dependent Variable: *Cybercrime in Selected Nigerian Deposit Money Banks*

Variables	Coefficient (β)	Std. Error	T-Value	P-Value
(Constant)	7.472	2.142	3.488	.001
FAS	.295	.132	2.111	.012
BS	.525	.121	4.351	.000
TI	.566	.124	4.559	.000
AGE	.093	.143	.652	.516

R= 0.648 $R^2 = 0.421$

Adjusted $R^2 = 0.402$ F-statistics = 23.205

P-value = 0.000000

Diagnostic Test			
	Test Statistics	P-Value	Decision
Normality of Residuals (Shapiro-Wilk)	0.983	0.072	Residuals are approximately normally distributed (p > 0.05)
Heteroskedasticity (Breusch-Pagan)	4.851	0.088	No evidence of heteroskedasticity (p > 0.05)
Autocorrelation (Durbin-Watson)	2.032	-	Residuals are independent; no autocorrelation

Source: SPSS Output (2026)

Table 4.6 presents the OLS regression results examining the effect of forensic accounting software (FAS), bank size (BS), technological investment (TI), and bank age (AGE) on cybercrime control (CCC) in selected Nigerian deposit money banks. The model demonstrates a good fit, with R = 0.648 and $R^2 = 0.421$, indicating that approximately 42.1% of the variation in cybercrime control is explained by the included predictors. The adjusted R^2 of 0.402 further confirms the explanatory strength of the model after adjusting for the number of variables. The F-statistic (23.205, $p < 0.001$) shows that the model is statistically significant overall, implying that the independent variables jointly have a significant effect on cybercrime control in the selected banks.

The a priori expectation for forensic accounting software (FAS), bank size (BS), technological investment (TI), and bank age (AGE) was that $\beta > 0$, indicating that these variables are expected to positively influence cybercrime control. The findings reveal that forensic accounting software has a positive and statistically significant effect on cybercrime control ($\beta = 0.295$, $t = 2.111$, $p = 0.012$). The finding aligns with the a priori expectation that forensic accounting software enhances fraud detection,

monitoring capabilities, and cybercrime prevention mechanisms in Nigerian deposit money banks; therefore, the null hypothesis is rejected. Similarly, the findings for bank size (β = 0.525, t = 4.351, p = 0.000) and technological investment (β = 0.566, t = 4.559, p = 0.000) align with the a priori expectation that larger banks and higher technological investments significantly improve cybercrime control through stronger financial capacity, advanced infrastructure, and improved digital security systems, leading to the rejection of their respective null hypotheses.

In contrast, bank age shows a positive but statistically insignificant effect on cybercrime control (β = 0.093, t = 0.652, p = 0.516). This finding does not align with the a priori expectation that older banks would have stronger cybercrime control systems due to accumulated experience and institutional development; hence, the null hypothesis is not rejected. The diagnostic tests further confirm the robustness of the model, as the Shapiro-Wilk test (p = 0.072) indicates normality of residuals, the Breusch-Pagan test (p = 0.088) shows no evidence of heteroskedasticity, and the Durbin-Watson statistic (2.032) confirms the absence of autocorrelation.

Effect of data mining tools on cybercrime in selected Nigerian deposit money banks

$$CCC_i = \beta_0 + \beta_1 DMT_i + \beta_2 BS_i + \beta_3 TI_i + \beta_4 AGE_i + \varepsilon_i$$

Table 8: Ordinary Least Square for Model II

Dependent Variable: *Cybercrime in Selected Nigerian Deposit Money Banks*

Variables	Coefficient (β)	Std. Error	T-Value	P-Value
(Constant)	4.235	2.022	2.094	.038
DMT	.323	.091	3.539	.001
BS	.386	.121	3.180	.002
TI	.497	.120	4.137	.000
AGE	.126	.136	.922	.358

R= 0.687 R^2 = 0.472

Adjusted R^2 = 0.455 F-statistics = 28.611

P-value = 0.00000

Diagnostic Test			
	Test Statistics	P-Value	Decision
Normality of Residuals (Shapiro-Wilk)	0.637	0.086	Residuals are approximately normally distributed (p > 0.05)
Heteroskedasticity (Breusch-Pagan)	3.293	0.063	No evidence of heteroskedasticity (p > 0.05)
Autocorrelation (Durbin-Watson)	3.184	-	Residuals are independent; no autocorrelation

Source: SPSS Output (2026)

Table 4.7 presents the OLS regression results examining the effect of data mining tools and technology (DMT), bank size (BS), technological investment (TI), and bank age (AGE) on cybercrime control (CCC) in selected Nigerian deposit money banks. The model demonstrates a strong fit, with R = 0.687 and R^2 = 0.472, indicating that approximately 47.2% of the variation in cybercrime control is explained

by the explanatory variables. The adjusted R^2 of 0.455 further confirms the model's explanatory strength after adjusting for the number of predictors. The F-statistic (28.611, $p < 0.001$) shows that the model is statistically significant overall, implying that the independent variables jointly have a significant effect on cybercrime control in the selected banks.

The a priori expectation for data mining tools (DMT), bank size (BS), technological investment (TI), and bank age (AGE) was that $\beta > 0$, meaning that these variables are expected to positively influence cybercrime control in Nigerian deposit money banks. The findings reveal that data mining tools have a positive and statistically significant effect on cybercrime control ($\beta = 0.323$, $t = 3.539$, $p = 0.001$). This finding aligns with the a priori expectation that the use of data mining tools enhances cybercrime control through improved detection of unusual transaction patterns, identification of suspicious behaviour, and early fraud warning systems; therefore, the null hypothesis is rejected. Similarly, the findings for bank size ($\beta = 0.386$, $t = 3.180$, $p = 0.002$) and technological investment ($\beta = 0.497$, $t = 4.137$, $p = 0.000$) align with the a priori expectation that larger banks and higher investment in technology significantly strengthen cybercrime control through improved infrastructure, better resource capacity, and advanced digital security systems, leading to the rejection of their respective null hypotheses.

In contrast, bank age shows a positive but statistically insignificant effect on cybercrime control ($\beta = 0.126$, $t = 0.922$, $p = 0.358$). This finding does not align with the a priori expectation that older banks would have stronger cybercrime control systems due to accumulated experience and institutional maturity; hence, the null hypothesis is not rejected. The diagnostic tests further confirm the reliability of the model, as the Shapiro-Wilk test ($p = 0.086$) indicates normality of residuals, the Breusch-Pagan test ($p = 0.063$) shows no evidence of heteroskedasticity, and the Durbin-Watson statistic (3.184) confirms the absence of autocorrelation, ensuring that the regression estimates are statistically robust and suitable for inference.

Discussion of Findings

This study provides valuable insights into the effects of forensic accounting practices and regulatory compliance investigations on cybercrime control in selected Nigerian deposit money banks. The discussion is based primarily on the results of the ordinary least squares regression analysis, while also triangulating evidence from secondary sources such as CBN reports, EFCC publications, NDIC fraud statistics, and audited financial statements. This triangulation strengthens the robustness of the findings by comparing empirical perceptions with documentary evidence from regulatory and industry reports.

The findings reveal that forensic accounting software (FAS) has a positive and statistically significant effect on cybercrime control in selected Nigerian deposit money banks ($\beta = 0.295$, $t = 2.111$, $p = 0.012 < 0.05$). This finding aligns with the a priori expectation that forensic accounting software enhances cybercrime detection and prevention through real-time monitoring and automated identification of suspicious transactions. It also confirms that banks adopting forensic accounting software are better positioned to detect anomalies, respond promptly to cyber threats, and reduce financial fraud. The result is further supported by secondary data evidence from CBN and EFCC reports, which indicate that banks with stronger digital forensic systems report improved fraud detection capabilities and faster response to cyber incidents. However, these same reports also show that cybercrime incidents persist in the banking sector, suggesting that effectiveness depends not only on adoption but also on depth of implementation and integration into broader control systems.

Theoretically, this finding is consistent with Technology Theory, which explains that the adoption of advanced technological systems enhances organizational efficiency, control, and risk management. The result also aligns with the Fraud Diamond Theory, which emphasizes that reducing opportunity through

technological monitoring systems weakens the likelihood of successful cyber fraud. Empirical support is provided by Olabisi (2024) and Ogunleye & Fanimokun (2025), who found that forensic accounting software significantly improves fraud detection and prevention in Nigerian banks. Similarly, Onourah and Appah (2022) affirm that forensic accounting tools reduce fraudulent activities by strengthening internal control systems. However, contrasting views by Gbegi and Adebisi (2024) and Owolabi et al. (2023) suggest that the effectiveness of forensic tools may be limited by inadequate implementation, insufficient training, and weak institutional support. This implies that while forensic accounting software is effective, its impact is conditional on proper integration and organisational readiness.

In addition, data mining tools and technology (DMT) positively and significantly influence cybercrime control in selected Nigerian deposit money banks ($\beta = 0.323$, $t = 3.539$, $p = 0.001 < 0.05$). This finding implies that banks that adopt advanced data mining and analytics systems are more capable of detecting unusual transaction patterns, identifying suspicious activities, and preventing cybercrime incidents before they escalate. The significant effect is attributable to the capacity of data mining tools to process large volumes of transactional data in real time, uncover hidden anomalies, and generate actionable insights that strengthen monitoring systems and enhance cyber risk management. Consequently, banks that invest in DMT are better positioned to improve cyber resilience, support regulatory compliance, and sustain customer confidence in digital banking services.

This finding aligns with the a priori expectation that data mining tools and technology enhance cybercrime control by improving early detection and prevention mechanisms within banking operations. It also supports the Inspired Confidence Theory, which argues that stakeholders' trust and confidence increase when organizations demonstrate effective systems for safeguarding assets and ensuring operational integrity. In this context, the deployment of data mining tools strengthens confidence among management, regulators, and customers that cyber risks are being actively monitored and controlled. Empirically, the result is consistent with Ole (2023) and Olabisi (2024), who found that digital analytics and data-driven tools significantly improve fraud detection and prevention in Nigerian deposit money banks. Similarly, Ogunleye & Fanimokun (2025) established that data mining systems enhance financial reporting quality and strengthen fraud management practices. However, contrasting evidence from Owolabi et al. (2023) and Gbegi & Adebisi (2024) suggests that the effectiveness of such tools may be constrained by inadequate technical skills, weak institutional enforcement, and poor system integration, indicating that the impact of DMT depends not only on adoption but also on organisational capacity and implementation quality.

Conclusion and Recommendations

The study examined the effect of forensic accounting practices and regulatory compliance investigations on cybercrime control in selected Nigerian deposit money banks. Drawing from the Fraud Diamond Theory, Agency Theory, and Space Transition Theory, the study provides evidence that cybercrime in the banking sector is largely driven by opportunity structures created within digital banking systems, agency conflicts, and the evolving nature of cyber environments. Empirical findings revealed that forensic accounting software and data mining tools exert a positive and statistically significant influence on cybercrime control. This suggests that advanced technological systems enhance banks' capability to detect anomalies, trace digital footprints, and identify fraudulent transaction patterns in real time. This outcome aligns with the Fraud Diamond Theory, which emphasizes that reducing opportunity and increasing detection capability significantly weakens the likelihood of successful cyber fraud. It also supports Space Transition Theory, which argues that cybercrime can be effectively controlled when institutions deploy strong monitoring systems that bridge the physical and

virtual environments where financial crimes occur. The study concludes that while regulatory compliance and audit mechanisms provide an essential governance foundation, they are not sufficient on their own to effectively combat cybercrime in deposit money banks. Instead, forensic accounting technologies and data-driven analytical tools represent the most effective mechanisms for strengthening cybercrime control. Therefore, the integration of advanced forensic systems into banking operations is critical for enhancing early detection, prevention, and response to cyber-related financial crimes in Nigeria's evolving digital financial environment.

The following recommendations were made:

i. Given that forensic accounting software was found to have a positive and statistically significant effect on cybercrime control, banks should prioritize the adoption, regular updating, and effective utilization of such software. Management should ensure that staff are adequately trained in forensic accounting tools to enhance early detection, monitoring, and investigation of fraudulent activities. Regular audits of software performance and integration with other monitoring systems can further improve its effectiveness, reducing cybercrime incidents.

ii. Banks should invest in advanced analytics platforms capable of detecting unusual transaction patterns, predicting potential threats, and monitoring electronic banking activities in real time. Staff should also be trained to interpret and act on insights from these tools, ensuring proactive cybercrime prevention.

References

Adeyemi, A., & Adebayo, T. (2023). Cybersecurity challenges and fraud control in Nigerian banking sector. *International Journal of Banking and Finance Research*, *9*(2), 45–62.

Akinyemi, O., & Adegbie, F. F. (2022). Data mining techniques and fraud detection in Nigerian financial institutions. *Journal of Accounting and Financial Management*, *18*(3), 112–129.

Amedu, C., & Nwankwo, O. (2022). Digital security systems and cybercrime prevention in Nigerian banks. *African Journal of Information Systems*, *14*(1), 33–50.

Bagozzi, R. P. (2007). The legacy of the technology acceptance model and a proposal for a paradigm shift. *Journal of the Association for Information Systems*, *8*(4), 244–254.

Bierstaker, J. L., Brody, R. G., & Pacini, C. (2024). Fraud detection tools and forensic accounting technologies. *Journal of Forensic Accounting Research*, *9*(1), 1–22.

CBN (Central Bank of Nigeria). (2023). *Annual report and statement of accounts*. Central Bank of Nigeria.

Choo, K. K. R. (2011). The cyber threat landscape and cybercrime control strategies. *Computers & Security*, *30*(8), 719–731.

Dada, S. O., Adekunle, J., & Olaniyi, T. (2023). Forensic accounting and fraud prevention in Nigerian banks. *International Journal of Accounting and Finance Studies*, *12*(2), 78–96.

Dorminey, J., Fleming, A. S., Kranacher, M. J., & Riley, R. A. (2012). The evolution of fraud theory. *Journal of Theoretical Accounting Research*, *7*(2), 15–43.

EFCC (Economic and Financial Crimes Commission). (2024). *Annual crime and fraud report*. EFCC.

Enofe, A. O., Omagbon, P., & Ehigiator, F. (2015). Forensic accounting and fraud detection in Nigerian banks. *International Journal of Business and Social Science*, *6*(3), 118–128.

Flint, D. (1988). Philosophy and principles of auditing. *Accounting, Auditing & Accountability Journal*, *1*(2), 1–15.

Gbegi, D. O., & Adebisi, J. F. (2024). Forensic accounting techniques and fraud detection in Nigeria. *Journal of Accounting and Taxation*, *16*(1), 55–74.

Hand, D. J., Mannila, H., & Smyth, P. (2001). Data mining in financial systems. *Statistical Science*, *16*(3), 111–133.

Hogan, C. E., Rezaee, Z., Riley, R. A., & Velury, U. (2008). Financial statement fraud: Insights from the academic literature. *Auditing: A Journal of Practice & Theory*, *27*(2), 33–59.

Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology? *Information & Management*, *40*(3), 191–204.

Limperg, T. (1932). The theory of inspired confidence. *Accounting History Review*, *2*(1), 1–20.

Ogunleye, O., & Fanimokun, J. (2025). Data mining tools and fraud prevention in Nigerian deposit money banks. *Journal of Financial Crime and Risk Management, 10*(1), 25–48.

Olabisi, S. O. (2024). Forensic accounting software and cybercrime control in Nigerian banks. *African Journal of Accounting and Auditing Research, 11*(2), 66–85.

Oladimeji, R., & Adegbie, F. F. (2023). Digital analytics and fraud detection in Nigerian banks. *Journal of Financial Innovation and Technology, 7*(1), 44–63.

Ole, S. (2023). Data analytics and fraud prevention in Nigerian deposit money banks. *International Journal of Digital Finance*, *5*(2), 90–108.

Onourah, J., & Appah, E. (2022). Forensic accounting and fraud detection in financial institutions. *International Journal of Accounting Research, 8*(1), 55–72.

Okoye, E. I., & Gbegi, D. O. (2023). Forensic accounting and fraud prevention in Nigerian banking sector. *Journal of Accounting and Finance Management, 9*(3), 101–120.

Porter, B. (1993). The audit expectation-performance gap. *Accounting and Business Research*, *23*(91), 49–63.

Singleton, T., & Singleton, A. (2020). Fraud auditing and forensic accounting systems. *Journal of Forensic & Investigative Accounting, 12*(1), 1–18.

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *CPA Journal, 74*(12), 38–42.