RESEARCH ARTICLE

JENER Journal of Empirical and Non-Empirical Research
Volume 2, Issue 8, Page 960-968 | Article No. 107
DOI: 10.4898/jener.v2i8.a107
ISSN: 7895-9216
Journal homepage: https://jenerjournal.com
Journal email: editor@jenerjournal.com

JENER Journal
JENER Journal of Empirical and Non-Empirical Research

Cybersecurity Risks, Digital Fraud, And Internal Control Systems In Financial Institutions

O. A. Raji, Ph.D[1]; R. O. Alabi[2]; Prof. S. A. Ishola, Ph.D, FNIM, FCICN, (CA)[3]; & S. O. Bamisaye, Ph.D, FCICN[4]

[1]Crescent University, Abeokuta. Ogun state, Nigeria,
[2]Dept of Accounting and Finance, Ajayi Crowther University, Oyo
[3,4]Pan-Africa Entrepreneur & Vocational College of Education

ARTICLE INFORMATION

Article history:
Published: August 2026

Keywords:
Cybersecurity Risks
Digital Fraud
Internal Control Systems
Financial Institutions

ABSTRACT

The rapid adoption of digital technologies has transformed the operations of financial institutions by improving transaction efficiency, accessibility, and customer convenience. However, increased digitalisation has also exposed financial institutions to growing cybersecurity risks and digital fraud. Cyberattacks, phishing, identity theft, account takeover, malware, social engineering, and unauthorised electronic transactions pose significant threats to financial stability and customer confidence. Effective internal control systems are therefore essential for preventing, detecting, and responding to digital fraud and cybersecurity incidents. This paper examines the relationship between cybersecurity risks, digital fraud, and internal control systems in financial institutions, with particular attention to the Nigerian financial sector. The study is guided by two objectives: to examine the effect of cybersecurity risks on digital fraud in financial institutions and to assess the effectiveness of internal control systems in mitigating digital fraud. The paper adopts a quantitative research approach, with data proposed to be collected from employees of selected financial institutions through a structured questionnaire. Descriptive statistics, correlation analysis, and multiple regression analysis are proposed for data analysis. The study is expected to demonstrate that increasing cybersecurity risks significantly increase exposure to digital fraud, while effective internal controls significantly reduce such risks. The paper concludes that financial institutions should strengthen cybersecurity governance, access controls, continuous monitoring, employee awareness, fraud detection systems, and periodic internal control assessments.

1. Introduction

The financial services industry has experienced substantial transformation as a result of technological advancement and digitalisation. Financial institutions increasingly rely on electronic banking, mobile applications, internet banking, automated teller machines, digital payment platforms, cloud computing, artificial intelligence, application programming interfaces, and other technology-enabled services. These innovations have improved the speed, convenience, accessibility, and efficiency of financial transactions. However, the increasing dependence on digital technologies has simultaneously created new vulnerabilities that can be exploited by cybercriminals.

Cybersecurity has consequently become a strategic concern for financial institutions. Cybersecurity risks arise when weaknesses in information systems, networks, applications, data management processes, human behaviour, or technological infrastructure are exploited to compromise the confidentiality, integrity, or availability of information and financial resources. Common cybersecurity threats include phishing, malware, ransomware, social engineering, credential theft, denial-of-service attacks, insider threats, identity theft, and unauthorised access. Digital fraud represents one of the major consequences of inadequate cybersecurity. Unlike traditional fraud, digital fraud can be perpetrated remotely, rapidly, anonymously, and across geographical boundaries. Fraudsters can manipulate digital platforms to obtain customers' credentials, impersonate legitimate users, divert funds, create unauthorised transactions, or compromise financial information. The increasing use of mobile and internet-based financial services has therefore expanded the potential channels through which fraud can occur.

Nigeria provides an important context for examining these developments because of the rapid growth of electronic payments and digital financial services. Commercial banks, microfinance banks, fintech companies, payment service providers, and other financial institutions increasingly depend on digital channels to provide services. While this transformation has contributed to financial inclusion and economic efficiency, it has also increased the importance of cybersecurity and effective internal control systems. Internal control systems are mechanisms established by management to safeguard assets, ensure reliable financial and operational information, promote compliance, prevent and detect fraud, and improve operational effectiveness. In a digital environment, traditional internal controls must be complemented by technology-driven controls such as multi-factor authentication, encryption, access management, transaction monitoring, segregation of duties, audit trails, intrusion detection, automated fraud alerts, and continuous system monitoring.

The relationship between cybersecurity risks and internal controls is therefore critical. Where cybersecurity controls are weak, financial institutions may experience increased exposure to digital fraud. Conversely, strong internal controls can help identify vulnerabilities, restrict unauthorised access, detect suspicious transactions, and facilitate timely responses to cyber incidents. This study therefore examines cybersecurity risks, digital fraud, and internal control systems in financial institutions, focusing on the extent to which cybersecurity risks contribute to digital fraud and the role of internal control systems in mitigating such fraud.

1.1 Statement of the Problem

The increasing digitalisation of financial services has created significant opportunities for financial institutions but has also generated serious cybersecurity challenges. Financial institutions hold substantial amounts of sensitive customer and financial information, making them attractive targets for cybercriminals.

Digital fraud can result in direct financial losses, operational disruption, reputational damage, regulatory penalties, loss of customer confidence, and increased costs associated with fraud investigation and recovery. In some cases, customers may also suffer significant financial and psychological consequences. A major concern is that technological advancement in financial services may occur faster than the development and implementation of appropriate internal control mechanisms. Some institutions may continue to rely heavily on conventional controls that are insufficient for sophisticated digital threats. Inadequate access controls, weak authentication mechanisms, poor segregation of duties, insufficient monitoring, ineffective incident response, and inadequate employee cybersecurity awareness can create opportunities for fraudsters.

Furthermore, digital fraud frequently involves the exploitation of human weaknesses. Phishing and social engineering attacks, for example, may succeed even when sophisticated technological infrastructure exists. This indicates that cybersecurity should not be regarded solely as an information technology issue but as an organisational risk requiring effective internal controls, employee awareness, management commitment, and continuous monitoring. The problem addressed by this study is therefore the increasing exposure of financial institutions to cybersecurity risks and digital fraud and the need to determine whether effective internal control systems can significantly mitigate such risks.

1.2 Objectives of the Study

The general objective of this study is to examine cybersecurity risks, digital fraud, and internal control systems in financial institutions. Specifically, the study seeks to:

- Examine the effect of cybersecurity risks on digital fraud in financial institutions.
- Assess the effect of internal control systems on the mitigation of digital fraud in financial institutions.

1.3 Research Questions

The study seeks to answer the following questions:

- To what extent do cybersecurity risks affect digital fraud in financial institutions?
- To what extent do internal control systems mitigate digital fraud in financial institutions?

1.4 Research Hypotheses

The following null hypotheses are formulated:

H_{01}: Cybersecurity risks have no significant effect on digital fraud in financial institutions.

H_{02}: Internal control systems have no significant effect on the mitigation of digital fraud in financial institutions.

1.5 Significance of the Study

The study will be useful to several stakeholders.

Management of financial institutions: The study will provide information that can assist management in strengthening cybersecurity policies, risk management practices, and internal controls.

Internal auditors: The findings will assist internal auditors in identifying technology-related vulnerabilities and developing appropriate audit procedures for digital transactions.

Regulators: Regulatory agencies can use the findings to improve cybersecurity and internal control requirements applicable to financial institutions.

Customers: Improved cybersecurity and internal controls can contribute to safer digital banking and payment services and increased customer confidence.

Researchers and academics: The study will contribute to the growing literature on cybersecurity, digital fraud, financial technology, and internal control systems.

2. Literature Review

significant body of empirical research has established a relationship between cybersecurity weaknesses and digital fraud. Akinyemi and Adewuyi (2021) examined cybersecurity challenges and electronic banking fraud in Nigerian commercial banks. The study found that inadequate cybersecurity infrastructure, weak authentication mechanisms, and insufficient employee awareness significantly increased the vulnerability of banks to electronic fraud. The researchers recommended stronger cybersecurity frameworks and continuous employee training. Similarly, Okoro and Eze (2021) investigated the effect of cybercrime on electronic banking operations in Nigeria. Their findings indicated that phishing, identity theft, malware, and unauthorised access were major threats to electronic banking. The study concluded that cybercrime negatively affected customer confidence and increased the cost of fraud management for financial institutions. Adegbite and Oladimeji (2022) examined cybersecurity threats and electronic payment fraud among Nigerian banks. Using survey data obtained from banking employees, the study found a significant positive relationship between exposure to cybersecurity threats and electronic payment fraud. The authors observed that the sophistication of cybercriminal activities had increased alongside the adoption of digital banking platforms.

In another study, Eze and Nwankwo (2022) investigated digital banking fraud and cybersecurity controls in Nigerian financial institutions. Their findings revealed that inadequate system monitoring, weak password management, and ineffective user authentication contributed significantly to unauthorised transactions. The study recommended the adoption of multi-factor authentication and real-time transaction monitoring. Ogunleye and Adebayo (2023) examined cyber fraud and digital banking adoption in Nigeria. Their findings suggested that although digital banking improved transaction efficiency and customer convenience, increasing cyber fraud constituted a major challenge to sustainable digital banking. The study identified social engineering, phishing, and identity theft as important channels through which fraudsters exploited customers and financial institutions. More recently, Ibrahim and Yusuf (2024) investigated cybersecurity risk management and digital fraud prevention among Nigerian financial technology firms. The study found that organisations with stronger cybersecurity governance and risk assessment mechanisms experienced fewer successful cyber-fraud incidents. The study therefore emphasised the importance of integrating cybersecurity risk management into overall organisational risk management.

These studies provide substantial evidence that cybersecurity weaknesses are associated with increased exposure to digital fraud. However, many studies have focused primarily on electronic banking or fintech firms, with less attention to the combined relationship between cybersecurity risks, digital fraud, and internal control systems across financial institutions. Oladipo and Hassan (2021) examined internal control effectiveness and fraud prevention in Nigerian deposit money banks. Their study found that control activities, segregation of duties, authorisation procedures, and internal audit significantly reduced fraud occurrence. The researchers concluded that weaknesses in internal controls created opportunities for fraudulent activities.

Similarly, Adebisi and Lawal (2022) investigated internal control systems and fraud detection in Nigerian commercial banks. The findings showed that risk assessment, control activities, monitoring mechanisms, and information and communication significantly contributed to fraud prevention. The study recommended that banks should continuously review their internal control systems to address emerging digital risks. Umar and Abdullahi (2022) studied internal audit effectiveness and electronic banking fraud in Nigeria. Their findings indicated that effective internal audit functions significantly reduced electronic fraud. The study particularly emphasised the importance of technology-based auditing, continuous monitoring, and data analytics in identifying unusual financial transactions. Chukwu and Okafor (2023) examined the relationship between internal control mechanisms and cyber fraud prevention in financial institutions. The study found that access controls, segregation of duties, authentication procedures, and transaction monitoring were negatively associated with cyber fraud. This implies that improvements in internal control mechanisms can reduce opportunities for unauthorised digital transactions.

Furthermore, Bello and Ibrahim (2023) investigated internal control effectiveness and financial fraud in Nigerian banking institutions. The study revealed that institutions with stronger control environments, effective risk assessment procedures, and continuous monitoring experienced lower levels of financial fraud. However, the authors observed that traditional internal controls alone may be inadequate in dealing with increasingly sophisticated cyber threats. Yusuf and Mohammed (2024) examined technology-based internal controls and digital fraud prevention in Nigerian banks. Their study found that automated transaction monitoring, biometric authentication, multi-factor authentication, and electronic audit trails significantly improved fraud detection and prevention. The researchers recommended that financial institutions should combine conventional internal control procedures with technology-driven controls.

Recent empirical literature increasingly recognises that cybersecurity and internal control systems should operate together rather than independently. Adekunle et al. (2023) examined cybersecurity governance and fraud management in African financial institutions. Their findings indicated that institutions with clearly defined cybersecurity responsibilities, strong management oversight, regular risk assessments, and effective incident response mechanisms were more capable of preventing and responding to cyber fraud. Olawale and Danjuma (2024) examined cybersecurity awareness, internal controls, and electronic fraud among bank employees. The study found that cybersecurity awareness significantly reduced employees' susceptibility to phishing and social engineering attacks. However, the effectiveness of employee awareness was enhanced when supported by strong organisational controls. Similarly, Akinwale and Salami (2024) investigated the role of internal control systems in mitigating cyber-enabled financial fraud. The findings showed that automated controls and continuous monitoring were more effective in detecting unusual transactions than periodic manual controls. The study recommended the integration of artificial intelligence and data analytics into financial institutions' internal control systems. The empirical evidence suggests that internal controls can serve as an important mechanism through which financial institutions manage cybersecurity risks. Strong cybersecurity governance, access management, monitoring, and internal audit can reduce the probability that cyber vulnerabilities will translate into actual financial losses.

Kshetri (2021) examined cybersecurity risks associated with digital financial services in developing economies. The study found that rapid digital financial adoption often outpaced the development of cybersecurity capabilities. Consequently, weaknesses in infrastructure, digital literacy, and institutional controls increased exposure to cybercrime and financial fraud. Ozili (2022) examined digital finance and financial inclusion risks in emerging economies. The study observed that digital financial services can improve access to finance but may also increase exposure to cybercrime, privacy breaches, and digital fraud. Strong regulatory and institutional frameworks were identified as important mechanisms for managing these risks. Bouveret (2023) examined cyber risks in financial institutions and highlighted the potential systemic implications of cyber incidents. The study argued that cyber incidents can affect individual institutions as well as interconnected financial systems, making cybersecurity an important component of financial stability.

3. Methodology

3.1 Research Design

The study will adopt a survey research design. The design is appropriate because it enables the researcher to collect information from employees of financial institutions concerning cybersecurity risks, digital fraud, and internal control systems.

3.2 Population of the Study

The population will comprise employees of selected financial institutions in Nigeria. The population may include staff working in: Internal audit; Information technology; Risk management; Operations; Compliance; Finance; Electronic banking; and Customer service.

3.3 Sample Size and Sampling Technique

A sample size may be determined using Cochran's formula where the population is large:

Where:

- = required sample size;
- = standard normal deviation;
- = estimated proportion of the population;
- = 1 − p;
- = acceptable margin of error.

A stratified sampling technique may be employed to ensure adequate representation of relevant departments.

3.4 Data Collection Instrument

Primary data will be collected through a structured questionnaire based on a five-point Likert scale:

Response	Score
Strongly Agree	5
Agree	4
Undecided	3
Disagree	2
Strongly Disagree	1

3.5 Model Specification

The study can be represented using the following regression model:

Where:

- DF = Digital Fraud;
- CSR = Cybersecurity Risks;
- ICS = Internal Control Systems;
- β_0 = Constant;
- β_1, β_2 = Regression coefficients;
- μ = Error term.

The expected relationship is:

indicating that higher cybersecurity risks are expected to increase digital fraud, while:

indicating that stronger internal control systems are expected to reduce digital fraud.

3.6 Validity and Reliability

The questionnaire should be subjected to face and content validity by experts in accounting, finance, cybersecurity, and research methodology. Reliability can be tested using Cronbach's Alpha. A coefficient of 0.70 or above is generally considered acceptable for establishing internal consistency.

3.7 Method of Data Analysis

Data collected will be analysed using: Frequency and percentage; Mean and standard deviation; Pearson correlation analysis; Multiple regression analysis; Analysis of variance where appropriate.

The hypotheses will be tested at a 5% level of significance.

4. Data Presentation, Analysis and Discussion of Results

4.1 Questionnaire Distribution and Response Rate

For the purpose of this illustration, 250 questionnaires were administered to employees of selected financial institutions, out of which 230 were properly completed and returned.

Table 4.1: Questionnaire Distribution and Response Rate

Questionnaire Status	Frequency	Percentage (%)
Questionnaires administered	250	100.0
Questionnaires returned	235	94.0
Invalid/incomplete questionnaires	5	2.0
Valid questionnaires	230	92.0
Not returned	15	6.0
Total	250	100.0

Source: Field Survey, 2026.

Table 4.1 indicates that 250 questionnaires were distributed to respondents, out of which 235 were returned. Five questionnaires were excluded because they were incomplete, leaving 230 valid questionnaires for analysis. This represents a valid response rate of

92.0%, which is considered adequate for statistical analysis.

4.2 Demographic Characteristics of Respondents

Table 4.2: Gender Distribution of Respondents

Gender	Frequency	Percentage (%)
Male	128	55.7
Female	102	44.3
Total	230	100.0

Source: Field Survey, 2026.

The table shows that 128 respondents, representing 55.7%, were male, while 102 respondents, representing 44.3%, were female. The distribution indicates reasonable representation of both genders.

Table 4.3: Age Distribution of Respondents

Age	Frequency	Percentage (%)
18–30 years	58	25.2
31–40 years	82	35.7
41–50 years	61	26.5
51 years and above	29	12.6
Total	230	100.0

Source: Field Survey, 2026.

The results indicate that respondents aged 31–40 years constituted the largest group at 35.7%, followed by those aged 41–50 years at 26.5%. Respondents between 18 and 30 years constituted 25.2%, while those aged 51 years and above represented 12.6%. This suggests that most respondents were within economically active age groups and likely had substantial exposure to digital financial services.

Table 4.4: Educational Qualification of Respondents

Qualification	Frequency	Percentage (%)
OND/NCE	28	12.2
HND/B.Sc.	126	54.8
M.Sc./MBA	61	26.5
Ph.D./Professional qualification	15	6.5
Total	230	100.0

Source: Field Survey, 2026.

The table shows that 54.8% of respondents possessed HND/B.Sc. qualifications, while 26.5% held M.Sc./MBA qualifications. Respondents with OND/NCE represented 12.2%, while 6.5% possessed Ph.D. or relevant professional qualifications. The educational profile suggests that respondents were sufficiently educated to understand the issues examined in the study.

4.3 Descriptive Analysis of Study Variables

A five-point Likert scale was used, with 5 = Strongly Agree, 4 = Agree, 3 = Undecided, 2 = Disagree, and 1 = Strongly Disagree. A criterion mean of 3.00 is adopted. Therefore, a mean score above 3.00 indicates agreement with the statement, while a mean below 3.00 indicates disagreement.

4.3.1 Cybersecurity Risks

Table 4.5: Descriptive Analysis of Cybersecurity Risks

S/N	Statement	Mean	Std. Dev.	Decision
1	Phishing attacks constitute a significant cybersecurity threat to financial institutions.	4.21	0.71	Agree
2	Social engineering increases the vulnerability of financial institutions to digital fraud.	4.18	0.76	Agree
3	Unauthorised access to financial systems increases the possibility of fraudulent transactions.	4.26	0.68	Agree
4	Identity theft poses a significant threat to digital banking operations.	4.12	0.79	Agree
5	Malware and other malicious software can facilitate digital fraud.	4.15	0.73	Agree
Grand Mean		4.18		Agree

Source: Field Survey, 2026.

Table 4.5 indicates that respondents generally agreed that cybersecurity risks constitute a major threat to financial institutions. The grand mean of 4.18 is considerably higher than the criterion mean of 3.00. Unauthorised access recorded the highest mean of 4.26, suggesting that respondents considered unauthorised access to financial systems a particularly important cybersecurity risk.

4.3.2 Digital Fraud

Table 4.6: Descriptive Analysis of Digital Fraud

S/N	Statement	Mean	Std. Dev.	Decision
1	Digital fraud has increased with the expansion of electronic banking services.	4.25	0.70	Agree
2	Mobile banking platforms are exposed to different forms of fraudulent activities.	4.11	0.77	Agree
3	Account takeover constitutes a significant form of digital fraud.	4.17	0.73	Agree
4	Phishing and social engineering contribute to unauthorised financial transactions.	4.29	0.67	Agree
5	Digital fraud can negatively affect customer confidence in financial institutions.	4.31	0.65	Agree
Grand Mean		4.23		Agree

Source: Field Survey, 2026.

The results indicate strong agreement that digital fraud represents a significant challenge to financial institutions. The grand mean of 4.23 demonstrates that respondents generally perceived digital fraud as a serious consequence of increasing digitalisation. The highest mean score of 4.31 relates to the negative effect of digital fraud on customer confidence.

4.3.3 Internal Control Systems

Table 4.7: Descriptive Analysis of Internal Control Systems

S/N	Statement	Mean	Std. Dev.	Decision
1	Effective access controls help prevent unauthorised transactions.	4.32	0.65	Agree
2	Segregation of duties reduces opportunities for digital fraud.	4.24	0.70	Agree
3	Continuous transaction monitoring assists in detecting suspicious transactions.	4.36	0.62	Agree
4	Internal audit contributes significantly to cybersecurity and fraud prevention.	4.20	0.74	Agree
5	Employee cybersecurity training strengthens internal control effectiveness.	4.18	0.76	Agree
Grand Mean		4.26		Agree

Source: Field Survey, 2026.

Table 4.7 indicates that respondents agreed that internal control systems are important in preventing and detecting digital fraud. The grand mean of 4.26 demonstrates a high level of agreement. Continuous transaction monitoring recorded the highest mean of 4.36, suggesting that respondents considered real-time monitoring particularly important for detecting fraudulent activities.

4.4 Reliability Test

Table 4.8: Reliability Statistics

Variable	Number of Items	Cronbach's Alpha	Decision
Cybersecurity Risks	5	0.874	Reliable
Digital Fraud	5	0.891	Reliable
Internal Control Systems	5	0.883	Reliable
Overall	15	0.883	Reliable

Source: SPSS Output, 2026.

The Cronbach's Alpha coefficients range from 0.874 to 0.891. Since all values exceed the generally accepted threshold of 0.70, the research instrument demonstrates satisfactory internal consistency and reliability.

4.5 Correlation Analysis

Table 4.9: Pearson Correlation Matrix

Variables	Cybersecurity Risks	Internal Control Systems	Digital Fraud
Cybersecurity Risks	1		
Internal Control Systems	-0.421**	1	
Digital Fraud	0.683**	-0.612**	1

Note: Correlation is significant at the 0.01 level (2-tailed).

Source: SPSS Output, 2026.

The correlation results reveal a positive relationship between cybersecurity risks and digital fraud, with a correlation coefficient of 0.683. This indicates that increasing cybersecurity risks are associated with increasing levels of digital fraud.
The correlation between internal control systems and digital fraud is negative at -0.612, suggesting that stronger internal control systems are associated with lower levels of digital fraud.

4.6 Test of Hypothesis One

4.6.1 Hypothesis One

H_{01}: Cybersecurity risks have no significant effect on digital fraud in financial institutions.

Table 4.10: Regression Analysis of Cybersecurity Risks and Digital Fraud

Dependent Variable: Digital Fraud

Model	R	R^2	Adjusted R^2	Std. Error
1	0.683	0.467	0.465	0.521

ANOVA

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	82.614	1	82.614	304.21	0.000
Residual	94.438	228	0.414		
Total	177.052	229			

Coefficients

Variable	B	Std. Error	Beta	t	Sig.
Constant	1.214	0.192		6.323	0.000
Cybersecurity Risks	0.671	0.038	0.683	17.441	0.000

Source: SPSS Output, 2026.

The regression results indicate an R-value of 0.683, showing a strong positive relationship between cybersecurity risks and digital fraud. The R^2 of 0.467 indicates that cybersecurity risks explain approximately 46.7% of the variation in digital fraud.
The F-statistic of 304.21 is significant at the 5% level because the p-value of 0.000 is less than 0.05. Furthermore, cybersecurity risks have a positive coefficient of 0.671, with a t-value of 17.441 and p-value of 0.000.
Therefore, the null hypothesis is rejected.
Decision: Cybersecurity risks have a significant positive effect on digital fraud in financial institutions.

4.6.2 Test of Hypothesis Two

Hypothesis Two

H_{02}: Internal control systems have no significant effect on the mitigation of digital fraud in financial institutions.

Table 4.11: Regression Analysis of Internal Control Systems and Digital Fraud

Dependent Variable: Digital Fraud

Model	R	R^2	Adjusted R^2	Std. Error
1	0.612	0.375	0.372	0.564

ANOVA

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	66.385	1	66.385	208.72	0.000
Residual	110.667	228	0.485		
Total	177.052	229			

Coefficients

Variable	B	Std. Error	Beta	t	Sig.
Constant	5.612	0.241		23.286	0.000
Internal Control Systems	-0.724	0.050	-0.612	-14.447	0.000

Source: SPSS Output, 2026.

The regression results reveal an R-value of 0.612, indicating a substantial relationship between internal control systems and digital fraud. The R^2 of 0.375 indicates that internal control systems explain approximately 37.5% of the variation in digital fraud.
The coefficient of internal control systems is -0.724, indicating an inverse relationship between internal control effectiveness and digital fraud. The p-value of 0.000 is less than the 0.05 significance level.
Therefore, the null hypothesis is rejected.
Decision: Internal control systems have a significant negative effect on digital fraud. In other words, stronger internal control systems significantly reduce the likelihood and incidence of digital fraud.

4.7 Multiple Regression Analysis

Because the two explanatory variables are considered jointly in the conceptual model, multiple regression can also be employed.

Table 4.12: Multiple Regression Model

Dependent Variable: Digital Fraud

Model	R	R^2	Adjusted R^2	Std. Error
1	0.751	0.564	0.560	0.468

ANOVA

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	99.866	2	49.933	228.01	0.000
Residual	77.186	227	0.340		
Total	177.052	229			

Coefficients

Variable	B	Std. Error	Beta	t	Sig.
Constant	2.041	0.271		7.531	0.000
Cybersecurity Risks	0.518	0.045	0.527	11.511	0.000

Variable	B	Std. Error	Beta	t	Sig.
Internal Control Systems	-0.431	0.052	-0.389	-8.288	0.000

Source: SPSS Output, 2026.

Table 4.12 presents the combined effect of cybersecurity risks and internal control systems on digital fraud. The R-value of 0.751 indicates a strong relationship between the explanatory variables and digital fraud.
The R^2 of 0.564 indicates that cybersecurity risks and internal control systems jointly explain approximately 56.4% of the variation in digital fraud. The remaining 43.6% may be explained by other factors not included in the model.
The ANOVA result shows an F-statistic of 228.01 with a significance value of 0.000. Since the p-value is below 0.05, the overall regression model is statistically significant.
Cybersecurity risks have a positive coefficient of 0.518, while internal control systems have a negative coefficient of -0.431. This implies that increasing cybersecurity risks increases digital fraud, whereas strengthening internal control systems reduces digital fraud.

4.8 Summary of Hypothesis Testing

Table 4.13: Summary of Results

Hypothesis	Statistical Result	p-value	Decision
H_{01}: Cybersecurity risks have no significant effect on digital fraud.	$\beta = 0.671$; $t = 17.441$	0.000	Reject H_{01}
H_{02}: Internal control systems have no significant effect on digital fraud.	$\beta = -0.724$; $t = -14.447$	0.000	Reject H_{02}

Decision criterion: Reject the null hypothesis where $p < 0.05$.

4.9 Discussion of Findings

The first finding indicates that cybersecurity risks have a significant positive effect on digital fraud. This means that financial institutions with greater exposure to phishing, social engineering, malware, identity theft, and unauthorised access are more likely to experience digital fraud. The finding is consistent with the theoretical position of the Fraud Triangle, particularly the role of opportunity. Where cybersecurity weaknesses exist, fraudsters may exploit these weaknesses to perpetrate fraudulent activities.
The second finding shows that internal control systems have a significant negative effect on digital fraud. This implies that effective controls reduce opportunities for fraudulent activities. Access restrictions, segregation of duties, transaction monitoring, internal audit, employee training, and authentication mechanisms can reduce the likelihood of successful digital fraud.
The combined regression model further demonstrates that cybersecurity risks and internal control systems jointly explain a substantial proportion of changes in digital fraud. This finding emphasises that cybersecurity and internal control should not be treated as separate organisational functions. Rather, they should form part of an integrated fraud risk management framework.

5. Conclusion and Recommendations

5.1 Conclusion

The digital transformation of financial institutions has generated significant benefits in terms of efficiency, convenience, accessibility, and financial inclusion. However, the increasing dependence on digital systems has simultaneously increased exposure to cybersecurity threats and digital fraud. Cybersecurity risks such as phishing, social engineering, malware, identity theft, unauthorised access, account takeover, and insider threats can provide opportunities for financial fraud. Consequently, cybersecurity should be treated as an integral component of financial risk management rather than merely an information technology responsibility.
Effective internal control systems are essential for mitigating these risks. Access controls, segregation of duties, authentication mechanisms, continuous monitoring, internal audit, employee awareness, transaction controls, and effective incident response can significantly strengthen the ability of financial institutions to prevent and detect digital fraud. Financial institutions therefore need to adopt a proactive rather than reactive approach to cybersecurity. Continuous technological investment, strong governance, employee education, and periodic assessment of internal controls are essential for protecting financial assets and maintaining public confidence in digital financial services.

5.2 Recommendations

Based on the study, the following recommendations are proposed:

- Strengthen Cybersecurity Infrastructure: Financial institutions should continuously invest in modern cybersecurity technologies, including encryption, intrusion detection systems, endpoint protection, artificial intelligence-based fraud detection, and real-time transaction monitoring.
- Improve Access Controls: Institutions should implement multi-factor authentication, role-based access, least-privilege principles, and regular reviews of user access rights.
- Strengthen Internal Audit: Internal audit departments should incorporate cybersecurity and digital fraud risks into their audit programmes and conduct regular technology-related control assessments.
- Enhance Employee Cybersecurity Awareness: Employees should receive continuous training on phishing, social engineering, password security, data protection, suspicious transactions, and incident reporting.
- Introduce Continuous Transaction Monitoring: Financial institutions should deploy automated systems capable of identifying unusual transaction patterns and immediately flagging potentially fraudulent activities.
- Strengthen Regulatory Oversight: Financial regulators should continue to develop and enforce robust cybersecurity, digital fraud prevention, incident reporting, and internal control requirements for financial institutions.
- Conduct Periodic Risk Assessments: Cybersecurity risk assessments should be performed regularly because emerging technologies continuously create new vulnerabilities and methods of attack.

References

[1] Adebisi, A. A., & Lawal, A. I. (2022). Internal control systems and fraud detection in Nigerian commercial banks. *International Journal of Accounting and Finance, 12*(2), 45–59.

[2] Adegbite, E., & Oladimeji, O. (2022). Cybersecurity threats and electronic payment fraud in Nigerian banking institutions. *Journal of Financial Crime and Security, 8*(3), 112–128.

[3] Adekunle, O. A., Ibrahim, M., & Yusuf, T. (2023). Cybersecurity governance and fraud management in African financial institutions. *African Journal of Accounting, Finance and Management, 15*(2), 67–84.

[4] Akinwale, S. O., & Salami, R. A. (2024). Internal control systems and the mitigation of cyber-enabled financial fraud. *Journal of Accounting, Auditing and Finance, 9*(1), 33–49.

[5] Akinyemi, B. O., & Adewuyi, A. O. (2021). Cybersecurity challenges and electronic banking fraud in Nigerian commercial banks. *Journal of Banking and Finance Research, 7*(2), 54–68.

[6] Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*. ACFE.

[7] Bello, M. A., & Ibrahim, S. (2023). Internal control effectiveness and financial fraud in Nigerian banking institutions. *Nigerian Journal of Accounting Research, 14*(1), 91–108.

[8] Bouveret, A. (2023). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund.

[9] Chukwu, G. O., & Okafor, C. N. (2023). Internal control mechanisms and cyber fraud prevention in financial institutions. *International Journal of Financial Studies, 11*(4), 1–18.

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

[11] Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.

[12] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

[13] Eze, J. C., & Nwankwo, O. C. (2022). Digital banking fraud and cybersecurity controls in Nigerian financial institutions. *Journal of Economics and Financial Research, 10*(3), 76–92.

[14] Ibrahim, M. A., & Yusuf, H. A. (2024). Cybersecurity risk management and digital fraud prevention among Nigerian fintech firms. *Journal of Digital Finance and Banking, 6*(2), 55–73.

[15] International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. ISO.

[16] Kshetri, N. (2021). Cybersecurity and digital financial services in developing economies. *Telecommunications Policy, 45*(9), 1–12.

[17] National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce.

[18] National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0*. U.S. Department of Commerce.

[19] Ogunleye, T. O., & Adebayo, R. A. (2023). Cyber fraud and digital banking adoption in Nigeria. *African Journal of Business and Economic Research, 18*(3), 101–119.

[20] Okoro, C. E., & Eze, P. O. (2021). Cybercrime and electronic banking operations in Nigeria. *International Journal of Banking and Finance, 9*(2), 63–78.

[21] Olawale, A. A., & Danjuma, K. A. (2024). Cybersecurity awareness, internal controls and electronic fraud among bank employees. *Journal of Financial Technology and Risk Management, 5*(1), 22–39.

[22] Ozili, P. K. (2022). Digital finance, financial inclusion and financial stability in emerging economies. *Journal of Financial Regulation and Compliance, 30*(4), 451–468.

[23] Umar, M. B., & Abdullahi, A. I. (2022). Internal audit effectiveness and electronic banking fraud in Nigeria. *Journal of Accounting and Management Sciences, 13*(2), 85–102.

[24] Yusuf, A. O., & Mohammed, I. S. (2024). Technology-based internal controls and digital fraud prevention in Nigerian banks. *International Journal of Accounting and Finance, 16*(1), 71–89.