THE INTERNATIONAL JOURNAL OF
BUSINESS & MANAGEMENT

Information Technology Control and Fraud Risk Assessment in Deposit Money Banks (DMBs) in Nigeria

Dada Samuel
Dean, Department of Management Sciences,
Babcock University, Ilishan-Remo, Nigeria
Ogundajo Grace
Lecturer, Department of Accounting,
Babcock University, Ilishan-Remo, Nigeria
Ohwo Onajero Kensington
Ph.D. Student, Department of Accounting,
Babcock University, Ilishan-Remo, Nigeria

Abstract:
The banking sector has been considered a fulcrum for economic growth in any country because of the intermediary role the banks play in collecting funds from the surplus household and giving it out at a markup to the deficit household. The operations of banks however had been faced with the risk of fraud which has led to the loss of a considerable amount of money running into billions of naira annually. Therefore, this study reviewed the effect of Information Technology Control on Fraud Risk Management in Deposit Money Banks (DMBs) in Nigeria.
The study employed the survey research design with a study population of 1,030. The 13 listed banks were used as samples for the study and the Taro Yamane formula was used to obtain a sample size of 288. The purposive sampling technique was subsequently used in administering the questionnaire to the respondents. The Cronbach-alpha reliability test coefficients ranged from 0.864 to 0.952. Descriptive and inferential statistics were used to analyze the data.
The results showed that IT control has a significant effect on fraud risk assessment in Deposit Money Banks (DMBs) in Nigeria with F287=51.818, Df = 3 & 264, adj. R2 =0.366, p-value=0.000< 0.05. The study concluded that IT Controls have a significant effect on fraud risk assessment in DMBs in Nigeria. The study, therefore, recommended that Banks should give priority to the implementation of information technology controls across all their digital channels or platforms as this will help to promote adequate fraud risk assessment and prevention on the platforms.

Keywords: *Information technology control, fraud risk management, application security control, fraud risk assessment*

1. Introduction

For any nation's economy to grow, it must have a robust banking system, this is because the banking system act as an intermediary between the surplus households that has so much money to save and the deficit households that need money to invest. The banking sector plays a major role in the development of any economy and it is the catalyst for growth (Nutanix, 2021; Ajala, Amuda, & Arulogun, 2013). Nevertheless, the sector suffers the occurrence of fraud globally (Desai, 2020; Mukhtaruddin, Sabrina, Hakiki, Saftiana, & Kalsum, 2020). Fraud has been in existence in banking and could be described as an act to deceive and take advantage of someone (Owolabi, 2010; Madan, 2016). According to the Association of Certified Fraud Examiners (ACFE, 2018) fraud is 'the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets.' Fraud has been defined differently by many authors but the common phrase in most of the definitions is 'deception'. Thus, fraud can also be defined as a deliberate act of deception intended at taking an unjustified advantage of someone (Gangwani 2020; Enofe, Abilogun, Omoolorun, & Elaiho, 2017).

A review of the Nigeria Deposit Insurance Corporation (NDIC) report for 2019 revealed that Card-related fraud {Automated Teller Machine (ATM)/Point of Sales (POS)} constituted the major fraud cases reported in the year, in line with the use of sophisticated modern-day technology techniques (Abilogun&Imagbe, 2017; Adetoso&Akinselure, 2016; Eneji, Angib, Ibe&Ekwegh, 2019). Fraud in the banking sector can be traced to the different channels or platforms or mediums used in carrying out transactions. These channels include mobile/internet banking channels, ATM, POS, Unstructured Supplementary Service Data (USSD), loan, cheque, and agent banking services (Idogei, Josiah &Onomuhara, 2017). A review of the FITC (2020) report on fraud and forgery in Nigerian banks reveals a systematic growth in the number of reported cases between Q1, Q2, Q3 & Q4 2020 as 18,326, 19,007, 27,347 and 28,692 respectively while the amount involved in the fraud cases are ₦8,399,594,513.28, ₦5,768,499,321.41, ₦9,190,356,953.37, ₦18,482,628,127.58

respectively. However, the actual loss amount for the four quarters is ₦719,481,364.71, ₦511,312,137.60, ₦2,634,689,219.06 and ₦1,806,543,799.62 respectively (FITC, 2020). Fraud is not limited to Nigeria rather it is a global occurrence (ACFE, 2018) which has led to the failure of multinational companies like Enron, Worldcom, NITEL (Adetoso & Akinselure, 2016; Olaoye & Dada, 2017).

Unlike the traditional internal control which has a multitude of researches that have been carried out on how fraud could be controlled using the traditional internal control measures, there seems to be a dearth of work in respect of information technology control and fraud risk management. The majority of the studies done so far in respect of information technology control and fraud were foreign. Usman and Mahmood, (2013) while examining critical factors that could prevent e-banking fraud itemized IT controls like biometrics, data encryption, authentication, and scalability of a security system but concluded that beyond the technology controls, there should be adequate customer awareness campaign and exposure to fraud preventative measures. Using big data technology as part of IT control in preventing fraud, Jianhao (2019) examined the effectiveness of the mechanism in curbing credit application fraud.

Given, the number of reported cases for the various fraud types and actual loss amount involved as enumerated, there is a need to curtail the menace, restore confidence in the banking sector by evaluating the various controls implemented to ascertain their effectiveness. Therefore, the objective of the study was to assess the effect of information technology control on fraud risk assessment in deposit money banks (DMBS) in Nigeria and the hypothesis for the study is stated as follows:

- $H_0$1: There is no significant effect of information technology control on fraud risk assessment in Deposit Money Banks (DMBs) in Nigeria.

1.1. Conceptual Review

1.1.1.. Fraud Risk Assessment

Fraud risk assessment has been defined in many ways, according to Mukhtaruddin et al, (2020), fraud risk assessment is the process of being proactively cautious about impending actions of the fraud minded people, private or corporate organizations. It entails being proactive in addressing fraud issues. It requires being active at all times in considering the vulnerabilities that the company is exposed to both from the inside and the external sources.

Kitteringham and Fennelly (2020) posited that fraud risk assessment is the recognition and identification of fraud risks, giving appropriate attention and priority to existing and potential fraud risks in an organization. It requires an active drive, education and communication risks to the organization. Fraud risk assessment has been defined in various forms by different studies. Duffin (2020), Mangala and Kumari (2015) defined fraud risk assessment as pragmatic and expert steps and precautions put in place to prevent fraud and make efforts to understand the vulnerabilities the companies are being exposed to fraud actions.

While Jesi and Desi (2019), Mukhtaruddin et al., (2020), Haoxiang and Smys (2021),Flowerastia, Trisnawati, and Budiono (2021) define fraud risk assessment as the ability to conduct a holistic and in-depth risk assessment and methodological verifications of the possible weak control measures to forestall occurrences of fraud, Basu (2020) noted that fraud risk assessment ought to start with all company employees irrespective of position, years in the service and extent of expertise of the employee. Yuswar-ZainalBasri (2020) further posited that a holistic and comprehensive understanding of how each employee interacts with each other and closeness during and after work is essential, especially for those entrusted with sensitive positions.

According to Mukhtaruddin et al., (2020), the complexities of fraud required that companies be active to scan the openness and integrity of staff handling products, and market exposure of the company, to prevent possible occurrences of staff taking undue advantage. Consistent with this view, Desai (2020) submitted that undue advantages can be abused and explored to perpetuate internal fraud. The senior and highly privileged employees ought to watch their conversations, communications within and outside the company premises concerning sensitive issues. Password to classified information should be carefully handled while access to some sensitive rooms is prohibited except for authorized employees (Enofe et al., 2017). External fraud risk can be attracted from external sources, particularly, where the organization's data and information issues are being managed by external consultants. Dubious staff could capitalize on any lapses and rake havoc against the company (Momani, Jamous&Hilles, 2017).

To determine the effectiveness of an organisation's fraud risk assessment program, measures such as data analytic procedure, employee survey, fraud risk scoring mechanism must be available as these are integral assessment tools (Alavi, 2016; Ernst & Young, 2016; COSO, 2016; Mpaata, Lubogoyi, &Okiria, 2017; Hussaini, Bakar, & Yusuf, 2019; Rehman & Hashim, 2020;Flowerastia et al., 2021; ACFE, 2021). Consequently, following the parameter used in the above-mentioned studies, this study measures fraud risk assessment using structured questions adopted from the studies of (Alavi, 2016; Ernst & Young, 2016; COSO, 2016; Mpaata, Lubogoyi, &Okiria, 2017; Hussaini, et al., 2019; Rehman & Hashim, 2020;Flowerastia et al., 2021; ACFE, 2021).

1.1.2. Information Technology Control

Businesses today rely on technology to serve their teaming customers. The Deposit Money Banks (DMBs) over the years has leveraged technology to reduce the crowd in the banking hall and enhance faster delivery of services. Since the technology employed has inherent risks, measures are put in place to guide against these risks. The measures put in place are the technology controls to assure that inherent risks are being mitigated. These measures are designed and implemented in the system or technology-enabled platforms to enhance the security and integrity of such platforms. Thus, IT controls help an organization mitigate the risk involved in the use of technology. These IT control measures include corporate policies, implementation of security codes, access restrictions, physical security, and automatic edits used in analyzing big data (Richards, Oliphant, & Le Grand, 2005).

Cram, Brohman, and Gallupe (2016) defined IT Control as an intentional act to manage the behaviour of persons or groups to design, operate, and manage information technology architecture. These controls are designed to ensure that the required technology is available when required and devoid of gaps that can be exploited by fraudsters. Uittenbogaard (2015) opined that

IT control is put in place to meet information security requirement objectives. These objectives are Confidentiality, Integrity, and Availability. While confidentiality serves to protect information from unauthorized access, integrity protects the actual value of the information from unauthorized modification and availability ensures that critical IT infrastructure is accessible when required.

IT control forms part of the broad spectrum of internal controls which plays a major role in the Sarbanes Oxley's Act of 2002 developed in the USA to prevent corporate fraud and corruption (Carter, Phillips, & Millington, 2012). IT control is further categorized into Application security control, Access control, and Network control.

1.2.Theoretical Framework

This study is anchored on the Technology Acceptance Model and Fraud Hexagon Theory.The Technology Acceptance Model (TAM) is an extension of the Theory of Reasoned Action (TRA) conceived by Fred Davis in 1986. The theory highlighted two technology acceptance measures (perceived usefulness and perceived ease of use) which replaced the Azjen and Fishbein TRA's attitude towards behaviour (Momani et al., 2017). In a simple term, the TAM explains the attitude of people to a new technological innovation in terms of the perceived usefulness of the novel technology (for example mobile banking application) and how easy they could use it. Lai (2017) defined perceived usefulness as the likelihood that an individual's use of a particular system or technology will boost his/her action while perceived ease of use is the extent to which the same individual requires the system or technology he is using to be effortless. However, Momani et al., (2017) opined that the design for TAM was done through three distinct stages: adoption, validation, and extension stages. The researchers further stated that at the adoption phase, the TAM was tested using a huge number of information technology applications and at the validation phase, TAM uses the correct measurement of user's acceptable behaviour in various applications while at the extension phase, new variables were introduced to determine the relationship between the TAM constructs.

One notable criticism of the TAM is that it did not contain the TRA's subjective/biased norms in its structures (Chuttur, 2013). Also, the TAM did not provide room for feedback on potential features that may enhance the acceptance like the currency of the information, flexibility, integration with other applications, and completeness of the information (Momani et al., 2017). However, Holden and Karsh (2010) in supporting the theory conducted a study on the use of TAM in predicting the use of acceptance of IT-enabled health applications. The result shows a positive relationship in which TAM predicts the usage of IT applications. The TAM will support this study as it will determine the level of users' acceptance of bank IT transaction platforms if the IT controls are effective in preventing or eliminating fraud associated with it. Thus, a high level of acceptance of bank technology-enabled applications symbolizes confidence in the applications and the need to use the right IT control to prevent fraud from occurring on the platforms.

The Fraud Hexagon theory like the Fraud Pentagon theory is an extension of the Fraud Triangle theory. The theory is also known as the SCCORE model where the acronym SCCORE stands for Stimulus, Capability, Collusion, Opportunity, Rationalization, and Ego. The new element in this theory is collusion which is an integral factor to commit fraud. The theory or model was postulated by Georgios (2019) in his work titled 'Advancing theory of fraud: The S.C.O.R.E. model'. He believed that once there is an avenue for people to collude, the possibility of committing fraud with all the other factors being in place is high. However, Kassem and Higson (2012) explain that to fully understand the causes of fraud, one theory alone is not sufficient to provide all but a study of the various theories on fraud will provide a more succinct view on the explanation of why fraud occurs.

In providing support for the fraud hexagon theory, YuswarZainalBasri and Zulhelmy (2020) conducted a study to determine how the theory predicts fraud intention in Zakat Management Company in Indonesia. The study concluded that the theory was able to effectively predict accounting fraud in the company. Similarly, Handoko and Tandean (2021) opined that pressure from external stakeholders, financial targets frequent changes of auditors, directors, and CEOs do not influence detection of fraud in financial statements of publicly listed companies.

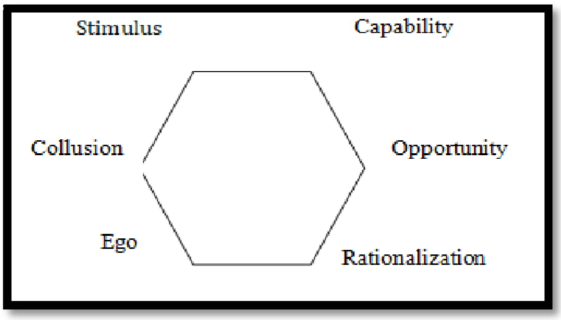

Figure 1: Fraud Hexagon theory
Source: Georgios (2019)

The fraud hexagon theory provides explanations for why people indulge in fraudulent activities. Each of the five enablers (stimulus, capability, collusion, opportunity, rationalization, and ego) of fraud provides a basic understanding of why fraud perpetrators behave the way they do, what motivates them and what factors, if available, could fuel the intent to commit the crime or fraud. The theory also provides understanding about the measures to put in place to ensure the five enablers of fraud are constrained or controlled to prevent fraud occurrence. Similarly, the Technology Acceptance theory provides an explanation and understanding of people's behaviour towards acceptance of technology-enabled bank platforms. This is necessary because the level of technology acceptance will determine usage, care for the application (Raman, 2011) as well as the use of the inbuilt controls to prevent fraud.

1.3. Empirical Review

The number of electronic fraud cases has been on the increase and this can be attributed to the increase in transactions on electronic banking terminals (NDIC, 2019). Several measures have been put in place to prevent electronic fraud. Some of these measures include the traditional internal control measures and IT controls. Idowu and Adedokun (2013) in a study opine that banks are not reluctant in implementing controls or reporting fraud cases to the regulators but that fraudsters get more sophisticated in their activities thereby leading to an increase in fraud cases. The study recommends that banks should implement traditional risk assessment measures such as periodic staff training, prosecuting indicted staff, maintenance of effective internal control and audit departments, and conducting adequate background checks for employees before appointments. The use of traditional internal risk assessment measures in preventing fraud is also supported by Ajala et al., (2013), Adetoso and Akinselure (2016), Udeh and Ugwu (2018), Idogei et al., (2017), Jesi and Desi (2019) in their different studies.

Disagreeing with the use of traditional risk assessment measures in combating fraud in the banking sector, Ion and Dragovic (2010) and Haoxiang and Smys (2021) advocate the use of technology controls and propose that secret camera be installed in the phone-enabled terminals to provide transmission of data securely and provide the required trust. They argued that this is necessary because of a lack of communication trust between the POS terminal and cardholders as they do not have means of authenticating the genuineness of the terminal. Aligning with the use of technology controls in preventing bank fraud especially ATM & POS fraud, Henniger and Nikolov (2011) propose the infusion of biometric verification on card transactions to strengthen the security and safeguard cardholders against fraud.

Hummel (2015) added that managing hardware and software inventory within the organization, embarking on secure configuration for all devices connected to the network, regular training of personnel, implementing access control based on 'need to know', and use of a secured network infrastructure help in preventing card terminal threats and fraud.

In a similar study on ways to safeguard POS and ATM used in restaurants, Collins (2013) finds that technologically enabled risk assessment medium such as the use of artificial intelligence like Aloha Restaurant Guard (ARG) is effective in discovering fraud and identifying employee unpalatable behaviours that could fuel security concerns as well as create an environment of accountability and fraud deterrence. Hines and Youssef (2019) support the use of technology-aided risk assessment measures such as artificial intelligence tools in preventing fraud. They find that machine learning (ML) techniques like neural networks, Random forest, Adaboost, and support vector machines are effective in assessing insider fraud in restaurant point-of-sales and ATM fraud. Relatedly, Kelly (2019) discovers that staff entrusted with POS operations have invented ways of using the terminal to defraud unsuspecting users of cardholders. He however disagreed with the use of only technology-enabled measures in assessing fraud risk and advocates a combination of technological and behavioural controls in properly assessing the risk of fraud caused by POS operators.

2. Methodology

The research method to be used in this study is the quantitative research method while the research design to be adopted for this study is the survey research design. The survey research design is considered appropriate and suitable for this study because it focuses on the opinions, beliefs, attitudes, judgment, and behaviour of people. The primary data used for this study was extracted from the questionnaires administered to selected bank officials who are knowledgeable about information technology control and fraud risk assessment in the DMBs in Nigeria.

2.1. Population

The population of this study consists of all DMBs in Nigeria as contained on the Central Bank of Nigeria Website. The geographical location for the study consists of 22 banks whose headquarters are situated in Lagos, Nigeria. The total number of DMBs as shown on the Central Bank of Nigeria website is twenty-two. A justification for selecting the banking sector as the anchor for this study is because of the role it plays as a financial intermediary in the economy by channeling funds from sufficient households to deficit households within the economy. Thus, the target population of the study was approximated to be 1,030 staff which were drawn from the Internal Audit, Internal Control, and IT departments of the 22 DMBs in Nigeria as shown in Table 1. This information was obtained from interaction with Human Resources.

No.	Banks	Population
1	Access Bank Plc.	60
2	Ecobank Transnational Incorporated	50
3	FBN Holdings Plc.	55
4	FCMB Group Plc.	55
5	Fidelity Bank Plc.	50
6	Guaranty Trust Bank Plc.	55
7	Stanbic IIBTC Holdings Plc.	45
8	Sterling Bank Plc.	45
9	Union Bank Nig. Plc.	60
10	United Bank For Africa Plc.	60
11	Unity Bank Plc.	50
12	Wema Bank Plc.	45
13	Zenith Bank Plc.	60
	Others	
14	Heritage Banking Co. Ltd	45
15	Globus Bank Ltd	45
16	Keystone Bank	40
17	Polaris Bank	35
18	Providus Bank	40
19	Standard Chartered Bank Nig. Ltd	40
20	SunTrust Nig. Ltd	45
21	Titan Trust Bank ltd	25
22	Citibank Nig. Ltd	25
	Total	1030

Table 1: Population of the Study
Source: Human Resources (2022)

2.2. Sample Size and Sampling Technique

The sample size for the study was 288 respondents. The sample size is determined using the Taro Yamane formula {n= N/{1+N(e)2}. Where n = sample size, N = population and e = margin of error.
n = 1030/{1 + 1030 (0.05)$^{2\}}$
n = 1030/.4
n = 288

Approximately 288 respondents in selected 13 banks that were listed in Nigeria as of 31st December 2020. A stratified sampling technique was used in the study to select the banks to get an adequate representation of the deposit money banks from the three categories of CBN license (International bank license, National bank license, and Regional bank license) in Nigeria. The purposive sampling technique was subsequently used in administering the questionnaire to the respondents because of the complex and busy schedule of bankers and the need to quickly retrieve administered questionnaires considering the tight time frame allocated for the study.

2.3. Model Specification

The model that was used in ascertaining the effects of the independent variables on the dependent variables of the study is specified as:
Y=*f*(X)
FRA = *f*(INFTC)
Y = Dependent Variable = Fraud Risk Assessment (FRA)
X = Independent Variable = Information Technology Control (INFTC)
Where
Y = y_1,
X = x_1, x_2, x_3

2.4. Functional Relationship

FRA = *f*(ASC, AAC, NSC) ………………………………………………(eqn.)

2.5. Regression Models

$FRA_i = \beta_0 + \beta_1 ASC + \beta_2 AAC + \beta_3 NSC + e_i$
Where:
ß$_0$ = Intercept u=R residual
e= Error Term
i = Cross sectional Variable
FRA = Fraud Risk Assessment
ASC = Application security control

AAS = Access/Authentication control
NSC = Network security control
INFTC = Information Technology Control

3. Data Analysis and Discussion of Finding

3.1. Analysis of Respondents' Responses

	Statements	SA	A	U	D	SD	Mean	Std. Dev.
1	The identification of risks considers internal factors such as the processes and controls in place to process and account for everyday transactions.	111 (38.7)	172 (59.9)	0 (0.0)	3 (1)	0 (0.0)	4.367	0.544
2	Data analytics is used to compile, display, and analyze the results of employee surveys, facilitated sessions, and other data-gathering techniques.	63 (22)	220 (76.7)	2 (0.7)	2 (0.7)	0 (0.0)	4.198	0.464
3	The fraud risk assessment team gathers information about potential fraud from internal sources, such as interviews with personnel, and complaints received from the whistleblowing platform,	124 (43.2)	162 (56.4)	0 (0.0)	1 (0.3)	0 (0.0)	4.425	0.516
4	Fraud risk assessment scoring matrix is used to identify and document the specific areas of greatest risk to the bank and help determine how to tailor the assessment process accordingly.	108 (285)	173 (60.3)	1 (0.03)	3 (1.0)	0 (0.0)	4.354	0.548
5	The Fraud risk assessment team obtains information from external sources such as industry news to understand the fraud risks and subset of risks specific to the bank.	133 (46.3)	150 (52.3)	0 (0.0)	0 (0.0)	0 (0.0)	4.470	0.499
6	The identification of risks does not consider internal factors such as the processes and controls in place to process and account for everyday transactions.	4 (1.4)	7 (2.4)	0 (0.0)	178 (62)	98 (34.1)	1.749	0.709
	Total Average Score						4.0	0.6

Table 2: Fraud Risk Assessment in DMBs in Nigeria
**Mean ≥ 4.0 = 'Satisfied', While **Mean≤ 2.0= 'Dissatisfied'*
Source: Research Work (2022)

Table 2 shows that 38.7% of the respondents strongly agreed that the identification of risks considers internal factors such as the processes and controls in place to process and account for everyday transactions, 59.9% equally agreed while 1% disagreed. On average, the respondents agreed (M=4.367, SD= 0.544). Similarly, the next item in Table 2 shows that 22% of respondents strongly agreed that data analytics is used to compile, display, and analyze the results of employee surveys, facilitated sessions, and other data-gathering techniques, 76.7% agreed, while 0.7% were both undecided and disagreed respectively. On average, respondents agreed that data analytics plays an important role in analyzing fraud data with an average mean of 4.198 and SD of 0.464.

Also, Table 2 shows that 43.2% of respondents strongly agreed that the fraud assessment team gathers information about fraud using the whistleblowing platform, 56.4% agreed while 0.3% disagreed. Overall, the respondent agreed that the whistleblowing platform has a positive effect on the fraud assessment process with an average mean of 4.425 and SD = 0.516. In the same vein, 28.5% of the respondents strongly agreed that the fraud assessment scoring matrix is used to identify specific areas of greatest risk to the bank, 60.3% agreed, 0.3% was undecided while 1% disagreed. On average, the respondents agreed (M=4.354, SD= 0.548). On how information is sourced, 46.3% of the respondents strongly agreed the Fraud risk assessment team obtains information from external sources such as industry news to understand the fraud risks and subset of risks specific to the bank, while 52.3% agreed. This shows that on average, the respondents agreed to the question with a mean = 4.470 and SD = 0.499. lastly, on the reverse question; identification of risks does not consider internal factors such as the processes and controls in place to process and account for everyday transactions, 1.4% of the respondents strongly agreed, 2.4% agreed but 62% disagreed while 34.1% strongly disagreed. On average, the respondents disagreed with the question with a mean = 1.749 and SD = 0.709. Overall, Table 2 shows that the respondents agreed that information technology control has an effect on the fraud risk assessment in DMBs in Nigeria. (M= 4.0, SD = 0.6). The analysis above clearly indicates that the DMBs prioritize fraud risk assessment. This is evidenced by the employment of various techniques (IT processes & controls, fraud risk scoring matrix, data analytics, reliance on multiple channels of information, specific and industry-wide factors, etc.) by the DMBs in their fraud risk assessment. It further shows that internal factors influence the occurrence of fraud within the bank. Hence, the internal structure of firms needs to be carefully designed to properly manage fraud risk.

3.2. Regression Tables for Hypothesis

Hypothesis one was tested using the multiple regression analysis. The data for information technology control (ASC, AAC and NSC) and fraud risk assessment were created by summing responses of all items for each of the variables. The results of the regression are presented in Table 3 below.

MODEL				
Variable	Coeff	Std. Err	T-Stat	Prob
Constant	0.789	0.267	2.953	0.003
ASC	0.396	0.062	6.354	0.000
AAC	0.126	0.058	2.180	0.030
NSC	0.267	0.054	4.927	0.000
R^2	0.373			
Adj R^2	0.366			
S.E of Reg.	0.194			
F-Stat	51.818			
Prob (F-Stat)	0.000			

Table 3: Regression Analysis for Model
Independent Variable: FRA
Source: Author's Work (2022)
Note: 5% Significance Level Was Adopted

Model

$FRA_i = \beta_0 + \beta_1 ASC_i + \beta_2 AAC_i + \beta_3 NSC_{i} + e_i$ …………………….Model
$FRA_i = 0.789 + 0.396ASC_i + 0.126AAC_i + 0.267NSC_i$

3.3. Interpretation

Hypothesis one of this study aimed to determine if Information Technology Control has a significant effect on Fraud Risk Assessment (FRA) in DMBs in Nigeria. Considering the signs of the estimated parameters, there exists a positive relationship between all the proxies of the independent variable (Application security control in DMBs in Nigeria (ASC), Access/Authentication control in DMBs in Nigeria (AAC), and Network Security Control in DMBs in Nigeria (NSC))and Fraud Risk Assessment in DMBs in Nigeria. This is represented by the signs of the coefficients β_1,β_2, and β_3 i.e., $0.396ASC_i$, $0.126AAC_i$, and $0.267NSC_i$ respectively.

This shows that 1% increase in ASC will lead to 40% increase in FRA, 1% increase in AAC will lead to 13% increase in FRA, 1% increase in NSC will lead to 27% increase in FRA. The value of the constant implies that if the independent variables employed do not exist, FRA would still maintain a positive value of 0.789.

The adjusted R^2 value of 36.6% for this model connotes the ability of all the independent variables to collectively explain about 37% variation in Fraud Risk Assessment. The remaining 63% is accounted for by other factors not included in this model. The comparison of the R^2 and adjusted R^2 implies that there is a good fit of the model.

Furthermore, Table 3 shows the results of regression analysis between information technology control and fraud risk assessment. The results on the table indicated that application security control (ASC) has a significant effect on fraud risk assessment in DMBs in Nigeria ($\beta1 = 0.396$, $t = 6.354$, $p= 0.000 < 0.05$), access/authentication control with ($\beta2 = 0.126$, $t=2.180$, $p=0.030 < 0.05$), and lastly, network security control with ($\beta3= 0.267$, $t= 4.927$, $p= 0.000 < 0.05$). The t-statistics reflects the individual significance of the variables in this model. It shows that all the proxies of the independent variable (Application security control in DMBs in Nigeria. (ASC), Access/Authentication control in DMBs in Nigeria (AAC), and Network Security Control in DMBs in Nigeria (NSC) had a significant relationship with Fraud Risk Assessment. The F-statistics measures the combined performance of all the independent variables on Fraud Risk Assessment. The F-statistics value for this model is 51.81. The significance of this F-statistics, depicted by the p-value of 0.00, which is less than the 5% level of significance adopted for this work shows that the combined proxies of Information Technology Control have a significant effect on Fraud Risk Assessment.

3.4. Decision

At the level of significance of 0.05, Degree of Freedom of 3 & 264, F-statistics of 51.81, adjusted R^2 of 0.366 and p-value of 0.0000 which is less than the 0.05 level of significance adopted for the study. Therefore, the null hypothesis for model one which states that 'Information technology control does not significantly affect Fraud Risk Assessment in

Deposit Money Banks (DMBs) in Nigeria' be rejected and the alternate hypothesis accepted with conclusion that 'Information Technology Control significantly affect Fraud Risk Assessment in DMBs in Nigeria.'.

4. Discussion of Findings

The findings of the study support the findings of Haoxiang and Smys (2021). The study being exploratory research disagreed with the use of traditional risk assessment measures in combating fraud in the banking sector. The study advocated the use of technology controls and propose that secret cameras be installed in the phone-enabled terminals to provide transmission of data securely and provide the required trust. The researchers argued that this is necessary because of a lack of communication trust between the POS terminal and cardholders as they do not have means of authenticating the genuineness of the terminal. The study, therefore, concluded that the information technology controls have a significant effect on fraud risk assessment in banks especially assessing fraud risk prevalent in the digital banking platforms (ATM, POS, online merchant platform, internet/mobile banking applications and agent banking applications). The study subsequently recommended that banks should invest in technology control to properly control fraud risk incidents. Relatedly, Hummel (2015) added that managing hardware and software inventory within the organization, embarking on secure configuration for all devices connected to the network are technology controls that aid fraud risk assessment processes.

The findings of the study also aligned with the study of Hines and Youssef (2019) that support the use of technology-aided risk assessment measures such as artificial intelligence tools in preventing fraud. The study finds that machine learning (ML) techniques like neural networks, Random forest, Adaboost, and support vector machines are effective in assessing insider fraud in restaurant point-of-sales and ATM fraud. Therefore, the current study implies that with adequate assessment of fraud risk, proper controls and measures will be implemented to prevent fraud occurrence. Also, with continuous assessments, even frauds that were hitherto not prevented will be detected and remediated to reduce the amount of loss.

The study also validated the findings of Kelly (2019) who discovers that staff entrusted with POS operations have invented ways of using the terminal to defraud unsuspecting users of cardholders. Although the researcher disagreed with the sole use of only technology-enabled measures in assessing fraud risk, it advocates a combination of technological and behavioural controls in properly assessing the risk of fraud caused by POS operators. Lastly, the findings of this study also corroborate the work of Collins (2013). Collins (2013) finds that technologically enabled risk assessment such as artificial intelligence like Aloha Restaurant Guard (ARG) is effective in discovering fraud and identifying employee unpalatable behaviours that could fuel security concerns as well as create an environment of accountability and fraud deterrence.

5. Conclusion

From the analysis conducted, it is evident that there is a significant effect of information technology control on fraud risk assessment in DMBs in Nigeria. This is manifested by the positive association that was found between the independent and the dependent variables through empirical analysis. In addition, the coefficient of determining the value that was gotten in the analysis affirmed the conclusion that information technology control has a significant effect on fraud risk assessment.

6. Recommendations

Emanating from the findings, conclusions and contributions of the study, the following recommendations are made:

Banks should give priority to the implementation of information technology control across all their digital channels or platforms as this will help to prevent the risk of fraud on the platforms.

Banks should enlighten and sensitize their customers on the controls built into digital channels to enable the customers to become aware, protect the controls and guard against abuse and compromise of the implemented IT controls.

The government through the CBN should review the adequacy of the information technology controls implemented in the banks during the examination conducted to ascertain the financial health of banks. This will help to address gaps discovered in the IT control architecture and measures put in place to address them appropriately.

The CBN should design a portal where bank customers can lodge their complaints independently with a notice automatically sent to the responsible bank. This will help the regulator to know precisely the number of fraud cases, medium, the amount involved and actual amount lost without moderation from the affected banks. Also, this will help the regulator to know the area where the fraud is prevalent and recommend the appropriate IT control guidelines to curb the fraud trend.

Deposit money banks should periodically review the adequacy of the implemented IT controls to ensure that they remain effective and working as designed. Also, since technology is evolving, the controls built into digital platforms or applications should be reviewed to ensure that they align with the technological changes.

7. References

i. Abilogun, O. T., &Imagbe, U. V. (2017). Determinants of internet banking fraud in Nigeria. Journal of Management Sciences, 15(7), 73-86.

ii. ACFE. (2018). Global study on occupational fraud and abuse.

iii. ACFE. (2018). Report to the nations. Asia-Pacific edition.

iv. ACFE. (2020). Report to the nations; 2020 global study on occupational fraud and abuse.

v. ACFE. (2021). Fraud risk management guide scorecard. Retrieved December 7, 2021, from Association of Certified Fraud Examiners: https://www.acfe.com/coso-scorecard.aspx?mode=input&principle=1

vi. Adetoso, A. J., &Akinselure, O. P. (2016). Fraud control and fraud prevention in Nigeria banking. International Journal of Research in Finance and Marketing, 6(12), 66-83.

vii. Ajala, A. O., Amuda, T., &Arulogun, L. (2013). Evaluating internal control system as preventive measure of fraud in the Nigerian banking sector. International Journal of Management Sciences and Business Research, 2(9), 15-22.

viii. Alavi, H. (2016). Mitigating the risk of fraud in documentary letters of credit. Journal of European Studies, 6(1), 139-156.

ix. Basu, I. (2020, August 26). India rattled by alarming rise in bank fraud. Retrieved November 9, 2020, from Asia Financial Times:
https://www.asiatimesfinancial.com/india-rattled-by-the-alarming-rise-in-bank-frauds#:~:text=According%20to%20the%20report%2C%20the,from%206%2C799%20the%20year%20before.

x. Carter, L., Phillips, B., & Millington, P. (2012). The impact of information technology internal controls on firm performance. Journal of Organizational and End User Computing, 24(2), 39-49.

xi. Chuttur, M. Y. (2013). Overview of the technology acceptance model: Origins, developments and future directions. Indiana University: Working Papers on Information Systems.

xii. Collins, G. (2013). Safeguarding restaurants from Point-Of-Sale fraud: an evaluation of a novel theft deterrent application using artificial intelligence. Journal of Hotel & Business Management, 2(1), 1-5.

xiii. COSO. (2016). Fraud risk management guide. Retrieved December 5, 2021, from
https://www.coso.org/documents/coso-fraud-risk-management-guide-executive-summary.pdf

xiv. Cram, W. A., Brohman, K., &Gallupe, R. B. (2016). Information systems control: A review and framework for emerging information systems processes. Journal of the Association for Information Systems, 17(4), 216-266.

xv. Desai, N. (2020). Understanding the theoretical underpinnings of corporate fraud. The Journal for Decision Makers, 45(1), 1-7.

xvi. Duffin, E. (2020, November 20). Malware and hacking attacks on ATM networks Europe 2014-2019. Retrieved February 14, 2021, from https://www.statista.com/statistics/707943/attacks-atm-hacking-malware-europe/

xvii. Eneji, E. S., Angib, U. M., Ibe, E. W., &Ekwegh, C. K. (2019). A study of electronic banking fraud, fraud detection and control. International Journal of Innovative Science and Research Technology, 4(3), 708-711.

xviii. Enofe, O. A., Abilogun, O. T., Omoolorun, J. A., &Elaiho, M. E. (2017). Bank fraud and preventive measures in Nigeria: An empirical review. International Journal of Academic Research in Business and Social Sciences, 7(7), 40-51.

xix. Ernst & Young. (2016). Implementing COSO's new fraud risk management guidelines. Retrieved December 5, 2021, from
https://na.eventscloud.com/file_uploads/92a257c28dbca2addab2e507d4f9c8dd_CS3-2-COSO-RyanHubbsVincentWalden.pdf

xx. FITC (2019). Report on Frauds & Forgeries in Nigerian Banks.

xxi. FITC (2020). Report on Fraud and Forgery in Nigerian Banks.

xxii. Flowerastia, R. D., Trisnawati, E., &Budiono, H. (2021). Fraud Awareness, Internal Control, and Corporate Governance on Fraud Prevention and Detection. Advances in Social Science, Education and Humanities Research, 570(1), 335-342.

xxiii. Gangwani, M. (2020). Suitability of forensic accounting in uncovering bank frauds in India: an opinion survey. Journal of Financial Crime, 28(2), 1-16.

xxiv. Georgios, V. L. (2019). Advancing theory of fraud: The S.C.O.R.E. model. Journal of Financial Crime, 26(1), 372-381.

xxv. Handoko, B. L., &Tandean, D. (2021). An Analysis of Fraud Hexagon in Detecting Financial Statement Fraud (Empirical Study of Listed Banking Companies on Indonesia Stock Exchange for Period 2017– 2019). 7th International Conference on E-Business and Applications, 93-100.

xxvi. Haoxiang, W., &Smys, S. (2021). A survey on digital fraud risk control management by automatic case management system. Journal of Electrical Engineering and Automation, 3(1), 1-14.

xxvii. Henniger, O., &Nikolov, D. (2011). Extending EMV payment smart cards with biometric on-card verification . 1-10.

xxviii. Hines, C., & Youssef, A. (2019). Class balancing for fraud detection in Point Of Sale systems. IEEE Conference Proceeding.

xxix. Holden, R. J., & Karsh, B.-T. (2010). The Technology Acceptance Model: Its past and its future in health care, Journal of Biomedical Informatics, 43(1), 159-172.

xxx. Hummel, R. (2015). Understanding and preventing threats to Point of Sale systems. SANS Institute, 2-28.

xxxi. Hussaini, U., Bakar, A. A., & Yusuf, M.-B. O. (2019). The effect of fraud risk management, risk culture and performance of banking sector: A conceptual framework. International Journal of Multidisciplinary Research and Development, 6(1), 71-80.

xxxii. Idogei, O. S., Josiah, M., &Onomuhara, G. O. (2017). Internal control as the basis for prevention, detection and eradication of frauds in banks in Nigeria. International Journal of Economics, Commerce and Management, 3(12), 724-736.

xxxiii. Idowu, A., &Adedokun, O. T. (2013). Evaluation of the effect of monitoring and control activities on fraud detection in selected Nigerian commercial banks. Research Journal of Finance and Accounting, 4(6), 57-63.

xxxiv. Ion, I., &Dragovic, B. (2010). Don't trust POS terminals!Verify in-shop payments with your phone. Create-Net, 1-10.

xxxv. Jesi, A. R., &Desi, A. (2019). Fraud risk factors and tendency to commit fraud: analysis of employees' perceptions. International Journal of Ethics and Systems, 1-18. doi:10.1108/IJOES-03-2019-0057

xxxvi. Jianhao, Y. (2019). Design and implementation of bank wind control anti-fraud project based on big data technology. Journal of Physics: Conference Series, 1-7.

xxxvii. Kassem, R., &Higson, A. (2012). The new fraud triangle model. Journal of Emerging Trends in Economics and Management Science., 3(3), 191.

xxxviii. Kelly, C. C. (2019). Experiential methods for identifying and reducing point of sale retail fraud. EDPACS, 59(5), 1-8.

xxxix. Kitteringham, G., &Fennelly, L. J. (2020). Handbook of Loss Prevention and Crime Prevention (Sixth Edition).

xl. Madan, L. B. (2016). Combating bank frauds by integration of technology: Experience of a developing country. British Journal of Research, 3(3), 221-233.

xli. Mangala, D., &Kumari, P. (2015). Corporate fraud prevention and detection: revisiting the literature. Journal of Commerce & Accounting Research, 4(1), 52-62.

xlii. Momani, A. M., Jamous, M. M., &Hilles, S. M. (2017). Technology acceptance theories: Review and classification. International Journal of Cyber Behavior, Psychology and Learning, 7(2), 1-14.

xliii. Mpaata, K. A., Lubogoyi, B., &Okiria, J. C. (2017). The effect of administrative controls on fraud detection and prevention in Barclays bank Uganda. International Journal of Science and Research, 6(2), 1079-1982.

xliv. Mukhtaruddin, Sabrina, E., Hakiki, A., Saftiana, Y., &Kalsum, U. (2020). Fraudulent financial reporting: fraud pentagon analysis in banking and financial sector companies. Issues in Business Management and Economics, 8(2), 12-24.

xlv. NDIC. (2018). Nigeria Deposit Insurance Corporation Annual Report.

xlvi. NDIC. (2019). Annual Report.

xlvii. Nutanix. (2021). What is application security? Retrieved June 20, 2021, from https://www.nutanix.com/info/what-is-application-security

xlviii. Olaoye , O. C., & Dada , A. R. (2017). The roles of auditors in fraud detection and prevention in Nigeria deposit money banks: Evidence from Southwest. European Scientific Journal November, 13(31), 290-306.

xlix. Owolabi, A. S. (2010). Fraud and fraudulent practices in Nigeria banking industry. African Research Review, 4(3), 240-256.

l. Raman, A. (2011). The usage of technology among education students in University Utara Malaysia: An application of extended Technology Acceptance Model. International Journal of Education and Development using Information and Communication Technology, 7(3), 4-17.

li. Rehman, A., &Hashim, F. (2020). Impact of Fraud Risk Assessment on Good Corporate Governance: Case of Public Listed Companies in Oman. Business Systems Research, 11(1), 16-30.

lii. Richards, D., Oliphant, A., & Le Grand, C. (2005). Information technology controls. The Institute of Internal Auditors.

liii. Udeh, N. S., & Ugwu, I. J. (2018). Fraud in Nigerian banking sector. International Journal of Academic Research in Business and Social Sciences, 68(5), 598-607.

liv. Uittenbogaard, F. (2015). Introduction seminar: Information and technology audit. The Hague, National Academy for Finance and Economics.

lv. Usman, A. k., & Mahmood, S. H. (2013). Critical success factors for preventing e-banking fraud. Journal of Internet Banking and Commerce, 18(2), 2-14.

lvi. YuswarZainalBasri, S., &Zulhelmy, T. (2020). S.C.C.O.R.E model to predict the accounting fraud intension. International Journal of Business and Management Invention, 9(10), 28-36.

Appendix

Questionnaire

Questionnaire on Information Technology Controls and Fraud Risk Assessment in Deposit Money Banks in Nigeria

Part 1: Personal Data

1. Kindly tick your gender, department, and highest academic qualification below?

Gender

Male □

Female □

Department

Internal Audit □

Internal Control □

Academic Qualification

Diploma □
Bachelor degree □
Master's degree □
PhD, Post-Doctoral □

Part 2: Section A = Fraud Risk Management; B = Information Technology Control

Dependent Variables

A-1: Fraud Risk Assessment in DMBs in Nigeria

	Statements	SA	A	U	D	SD
1	The identification of risks considers internal factors such as the processes and controls in place to process and account for everyday transactions.					
2	Data analytics is used to compile, display, and analyze the results of employee surveys, facilitated sessions, and other data-gathering techniques.					
3	The fraud risk assessment team gathers information about potential fraud from internal sources, such as interviews with personnel, and complaints received from the whistleblowing platform,					
4	Fraud risk assessment scoring matrix is used to identify and document the specific areas of greatest risk to the bank and help determine how to tailor the assessment process accordingly.					
5	The Fraud risk assessment team obtains information from external sources such as industry news to understand the fraud risks and subset of risks specific to the bank.					
6	The identification of risks does not consider internal factors such as the processes and controls in place to process and account for everyday transactions.					

Table 4

B. Independent Variables

B-1: Application security control in DMBs in Nigeria.

	Statements	SA	A	U	D	SD
1	Transaction limit controls are built into applications developed by the bank to manage fraud					
2	Authorization limit controls are built into web and mobile applications developed by the bank					
3	Mobile and web applications deployed have validation check capability to ensure the accuracy of transactions.					
4	Applications developed have real-time rule base capability to prevent unauthorized fraudulent transactions.					
5	Regular reviews are conducted to determine the effectiveness of the transaction limit and authorization controls.					
6	Transaction limit controls are not built into applications developed by the bank					

Table 5

B-2: Access/Authentication control in DMBs in Nigeria.

	Statements	SA	A	U	D	SD
1	Biometric access control has been implemented in the bank's mobile and web applications to prevent unauthorized transaction					
2	Critical and sensitive areas in my bank can only be accessed by the use of biometric access installed on the doors.					
3	Physical access control is implemented to complement biometric access control in my bank					
4	There is an adequate budget to support the implementation of biometric access control and physical access control.					
5	Technically skilled staff are available to resolve identified challenges or problems with biometric access locks.					
6	Biometric access control has not been implemented in the bank's mobile and web applications.					

Table 6

B-3: Network Security Control in DMBs in Nigeria

	Statements	**SA**	**A**	**U**	**D**	**SD**
1	My bank has implemented a firewall across all network points to allow only authorized access to the bank network					
2	An intrusion Prevention System (IPS) has been implemented to prevent unauthorized access to the bank network					
3	An intrusion Detection System (IDS) is implemented in my bank to detect unauthorized access to the bank network.					
4	There is an adequate budget to support the implementation of firewall, IPS and IDS.					
5	The implemented firewall, IDS and IPS is reviewed periodically to ensure they remain effective and adequate.					
6	My bank has not implemented a firewall across all network points to allow only authorized access to the bank network					

Table 7

[(SA= Strongly Agree; A = Agree; U = Undecided D = Disagree; SD = Strongly Disagree).
Adapted and Modified: From the studies of (COSO, 2016; Sabani&Rishan, 2019; Zainal et al., 2017; Flowerastia et al., 2021; Haoxiang and Smys 2021;ACFE, 2021; Aladejebi and Oladimeji (2019);Otero, 2019;