INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

*ISSN 2278 – 0211 (Online)*

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

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

***Abstract:***
*The banking sector has been considered as a fulcrum for economic growth in any country because of the intermediary role the banks play in collecting funds at interest from the surplus household and giving it out at a markup to the deficit household. The smooth 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. This challenge had brought a bigger problem of how to properly manage the risk of fraud and boast customers' confidence in the banking sector in Nigeria and globally. Information Technology Control had been perceived to influence fraud risk management. Therefore, this study reviewed the effect of Information Technology Control on Fraud Risk Detection in Deposit Money Banks (DMBs) in Nigeria.*
*The study employed the survey research design with a study population of 1,030 which comprised staff in the Internal Control, Internal Audit and Information Technology departments of all Deposit Money Banks (DMBs) in Nigeria as contained on the CBN website. 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 reliability of Cronbach-alpha coefficients ranged from 0.864 to 0.952. Descriptive and inferential statistics were used to analyze the data.*
*Similarly, the study showed that IT control has a significant effect on fraud risk detection in Deposit Money Banks (DMBs) in Nigeria with* $F_{287}$*=30.690, Df = 3 & 265, adj.* $R^2$ *=0.209, p-value=0.000< 0.05. The study, therefore, concluded that IT Controls have a significant effect on fraud risk detection 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 detection on the platforms and boost customers' confidence in the banking sector.*

***Keywords:*** *Information technology control, Fraud risk assessment, fraud triangle theory*

## 1. Introduction

The banking system plays a major role in the development of any economy by accelerating economic development (Nutanix, 2021; Ajala, Amuda, & Arulogun, 2013). The evolution of the banking sector over the years from the manual traditional system of banking to a more advanced technology-driven system of banking has introduced complex fraud that is negatively affecting the operations of the banks (Desai, 2020; Mukhtaruddin, Sabrina, Hakiki, Saftiana, & Kalsum, 2020). Fraud is as old as banking and could be described as an act to deceive and take advantage of someone (Owolabi, 2010; Madan, 2016). The Association of Certified Fraud Examiners (ACFE, 2018) describe fraud as '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'. This means any deliberate act of deception that is intended at taking an unjustified advantage of someone can be described as fraud.

Fraud is global and not limited to a particular continent or country (Mukhtaruddin et at., 2020; Desai, 2020). Some studies from advanced economies have made tremendous attempts considering fraud detection. For instance, the studies of (Yazici, 2020; Basu, 2020; Yuswar-ZainalBasri, 2020; Kariapper, Razeeth, Pirapuraj and Nafrees 2020; Gangwani, 2020; Mukhtaruddin et al., 2020; Madinakhon, Dildora, Shohsanam, & Dilnoza, 2019; Momani, Jamous&Hilles, 2017). The world bank in collaboration with the International Monetary Fund (IMF) in the mid-1990s devised a strategy called the Financial Sector Assessment Program (FSAP) to combat different types of fraud in order to curb the global rising fraud scourge

which has affected many nations (Madinakhon et al., 2019). Findings from the KPMG (2019) global fraud survey show that more than half of the respondents globally encountered increases in cases and value of external fraud. Other findings by the KPMG survey show that over 25% of fraud-related losses were recovered with the aid of technology-enabled measures like machine learning real-time fraud alert, facial, voice & thumbprint recognition, and behavioural biometrics which profile how customers interact with their devices and internet banking. One significant finding from the KPMG global survey is that in every region, the banks surveyed considered cyber attacks as the most significant challenging fraud risk. This means that more efforts are required to curtail the cyberattack risk. Of the 43 retail banks that participated in the global banking fraud survey, 13 are in the Asia-Pacific, 5 in America, 25 in Europe, the Africa region, and the Middle East.

The Nigeria banking sector is not left out of the fraud risk scourge raving the global economy. 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 are ₦719,481,364.71, ₦511,312,137.60, ₦2,634,689,219.06 and ₦1,806,543,799.62 respectively (FITC, 2020).

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.

Therefore, since the number of reported cases of fraud and the actual loss amount involved is increasing, there is a need to curtail the menace and restore confidence in the banking sector by evaluating the various controls implemented to ascertain their effectiveness.

The objective of the study, therefore, was to assess the effect of information technology control on fraud risk detection in deposit money banks (DMBS) in Nigeria and the hypothesis for the study is stated as follows:

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

*1.1. Conceptual Review*

Fraud risk detection is defined as the process of knowing early signs of fraud risk that is about to happen (Idogei, Josiah &Onomuhara, 2017; Haoxiang and Smys, 2021). It allows early uncovering and recognition of tendencies and appearance of fraud in an organization, where proactive measures as tools alert the organization of potential fraud by the employee or an intruder, hackers and cybercriminals. In recent times, security software is deployed to raise alerts when there are attempts of fraudulent activity in the system. The software communicated any anomalies and the staff on alert be well informed of the early warning and any waiting signs based on the in-built signalling measures to raise red-flag (Kolapo &Olaniyan, 2018). According to Rubasundram (2019), early reporting of suspected fraud signals is imperative and one of the pillars of early fraud detection, and also such reports must not be sketchy, but promptly detailed and made available to the appropriate person who will take action.

Flowerastia, Trisnawati, and Budiono (2021)opined that one important fraud detection measure is the use of whistleblowing platforms where employees can escalate or report fraudulent activities that have crystallized. The medium enables management to act or respond to fraudulent actions and take corrective measures to salvage or reduce the loss amount as well as unravel the perpetrators and prosecute them to serve as a lesson to other staff or individuals as the case may be. Other measures to detect fraud include effective internal audit reviews and investigation, data analytic mechanisms and feedback mechanisms (Alavi, 2016; Ernst & Young, 2016; COSO, 2016; Mpaata, Lubogoyi, &Okiria, 2017; Hussaini, Bakar, & Yusuf, 2019; ACFE, 2021; Flowerastia et al., 2021). Consequently, following the parameter used in the above-mentioned studies, this study measures fraud risk detection using structured questions adopted from the studies of (Alavi, 2016; Ernst & Young, 2016; COSO, 2016; Mpaata et al., 2017; Hussaini et al., 2019; ACFE, 2021; Flowerastia et al., 2021)

Time and date, what really went wrong must be reported and such report must be well documented and stored in sensitive areas. Where fraud is detected, there must be a detailed investigation a systemic measure known by all as to the modalities of reporting any suspected fraud and made to raise a red flag and if possible a reward system be instituted to honest employees and those who raise an accurate alarm (Ernst & Young, 2016).

*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.

## 2.Theoretical Framework

*2.1.Technology Acceptance Model*

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 in the platforms.

*2.2. Fraud Hexagon Theory*

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) opine that pressure from external stakeholders, financial targets frequent change of auditors, directors, and CEOs do not influence detecting fraud in financial statements of publicly listed companies.

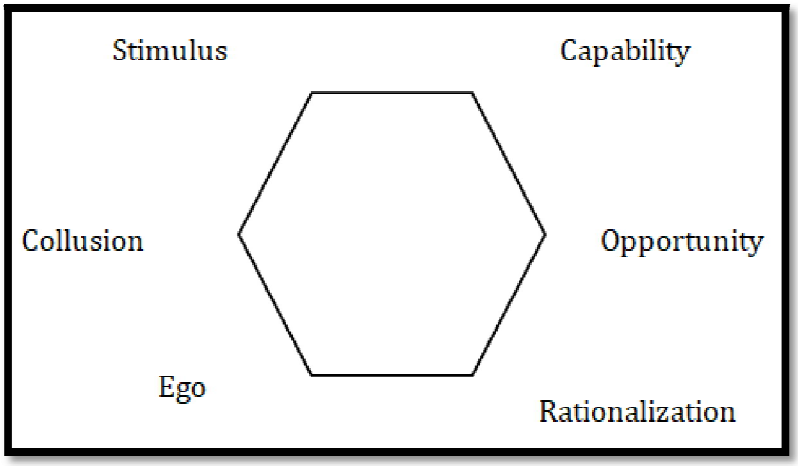


*Figure 1: Fraud Hexagon Theory*

The study is however anchored on the TAM and fraud hexagon theories. This is because while 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.

*2.3. Empirical Review*

The introduction of e-banking platforms where customers can easily access loans without having to go through the rigour of physically being present at the banking has made loan fraud detection complicated (Fadayo, 2018). In a bid to solve the fraud prevention and detection challenge, Okokpujie, John, Chinyere, Anele, Olajide (2016), and Albashrawi (2016) propose the use of data mining techniques that will learn the pattern of customers' transactions that can lead to fraud and stop it before it occurs. The study concludes that fraud detection will save the banks from huge losses resulting from fraud if it is a nip in the bud. Mousa (2016), Amanze and Onukwugha (2017) support the use of data mining techniques which is a known application control measure to prevent loan fraud because it is robust enough to detect sophisticated fraud, minimize loss, and scalable to manipulate the large volume of data.

Relatedly, Jianhao (2019) advocates the use of big data to solve the fraud problem but Jeyanthi, Mansurali, Harish and Krishnaveni (2020) opine that the data mined should be critically analyzed to provide patterns that could be useful in preventing e-banking fraud. However, Ajah and Inyiama (2011) and Cai and Zhu (2016) advocated the use of advanced technology such as blockchain technology by banks to reduce fraud losses and receive a commensurate level of return for shareholders.

In contrast, Xie et al., (2019) find that the current engineering solution that is dependent on the data mining technique is not adequate to detect fraud, rather recommend a rule-based solution that considers both individual transaction and group transaction patterns, and portrays the individual transaction as group solution which can adequately differentiate legitimate transactions from fraudulent ones. An earlier study by Saia, Boratto, and Carta (2015) adopts multiple behavioural models to learn and understand electronic bank users' transaction patterns to detect fraudulent transactions. Similarly, Li, Liu, Wang, Xuan, and Jiang (2018) explore the use of the Kernel-Based Supervised Hashing techniques to solve the fraud problem facing e-banking applications. The KSH is a technique used to detect credit card fraud by using past genuine transactions to predict future fraudulent transactions.

However, Zheng, Liu, Yan, and Jiang (2018), Ogbonna, Okaro, and Igwe (2019) queried the use of behavioural analysis in preventing fraud and highlighted the flaws in the existing fraud detection technique that uses the behaviour profile of customers to analyze their transactions to detect fraudulent ones. The study revealed that with the dynamism in customers' transactions across the internet, the existing behaviour profile technique is not capable of detecting fraud from this medium but proposed the use of Logical Graph of Behaviour Profile (LGBP) which has the capability of detecting fraud across different transaction platforms. This is because the LGBP is a total order-based model which represents the logical features of transaction records. Similarly, Luhach, Dwivedi, and Jha (2014) criticized the behavioural model and claimed that the security architecture built into many current e-commerce applications is not adequate because they are poorly designed and proposed the use of Security Oriented Architecture model that uses logical security to solve the fraud problem.

Other scholars believe the fraud scourge can be properly managed using a non-technology traditional approach. Zuraidah, Mohd, and Yusarina (2015) argued that full compliance with regulatory guidelines in terms of risk management and internal control is vital to preventing fraud in banks. The study concludes that fraud occurs due to loopholes in controls and thus, banks should address all weaknesses in their internal control system. While supporting this view, Ashamu (2014) and Dubey and Manna (2015) discover that fraudsters are becoming more skilful in committing fraud and

recommend that banks should implement strong fraud risk management and traditional control mechanism to detect and curb the fraud trend. In a related case, in studies to determine the effect of forensic accounting in preventing fraud in Nigeria banks, Ezejiofor, Nwakoby and Okoye (2016), Alao (2016), and Ogundana, Okere, Ogunleye, and Oladapo (2018) found that forensic accounting is an adequate tool in detecting the fraud scourge in the banking sector. However, Okonkwo and Ezegbu (2016) and Aladejebi and Oladimeji (2019) argued that the traditional internal control mechanism employed by banks have not been adequate in detecting fraud and suggested that banks should create ethics unit and reduce over-reliance on their staff. But Peters, Richardson, and Watson (2012) opine that firms with material IT gaps in their financial reporting system are associated with inaccurate management estimates than the estimates for firms that do not have material IT gaps in their financial reporting system.

## 3.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 detection in the DMBs in Nigeria.

### *3.1. 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 human resources as indicated in Table 1.

| 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)*

### *3.2. 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.

*3.3. 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)

FRD = *f*(INFTC)

Y = Dependent Variable = Fraud Risk Detection (FRD)

X = Independent Variable = Information Technology Control (INFTC)

Functional Relationship

FRD = *f*(ASC, AAC, NSC) .....(eqn. 1)

Regression Models

$FRD_i = \beta_0 + \beta_1 ASC + \beta_2 AAC + \beta_3 NSC + e_i$

Where:

$ß_0$ = Intercept u=R residual

e= Error Term

*i* = Cross sectional Variable

FRP = Fraud Risk Detection

ASC = Application security control

AAS = Access/Authentication control

NSC = Network security control

INFTC = Information Technology Control

## 4.Data Analysis and Discussion of Finding

*4.1. Analysis of Respondents' Responses*

| | Statements | SA | A | U | D | SD | Mean | Std. Dev. |
|---|---|---|---|---|---|---|---|---|
| 1 | There is whistle blowing mechanism in place to enable employee report identified fraud | 124 (43.2) | 151 (52.6) | 4 (1.4) | 0 (0.0) | 1 (0.3) | 4.379 | 0.631 |
| 2 | Data analytic procedures is implemented to trigger follow-up investigations of fraudulent transactions | 81 (28.2) | 201 (70) | 3 (1.0) | 2 (0.7) | 0 (0.0) | 4.258 | 0.505 |
| 3 | Regular review of transactions using application controls are conducted to detect fraudulent ones | 138 (48.1) | 148 (51.6) | 0 (0.0) | 1 (0.3) | 0 (0.0) | 4.474 | 0.5207 |
| 4 | The internal audit team reviews application controls, investigate all fraud allegations and develops an appropriate work plan accordingly. | 125 (43.6) | 159 (55.4) | 0 (0.0) | 0 (0.0) | 0 (0.0) | 4.440 | 0.497 |
| 5 | The internal audit team performs investigations using applicable professional standards and are free from any conflicts of interest | 175 (61) | 111 (38.7) | 0 (0.0) | 0 (0.0) | 0 (0.0) | 4.612 | 0.4882 |
| 6 | A whistleblowing mechanism is not in place to enable employees to report identified fraud | 4 (1.4) | 8 (2.8) | 5 (1.7) | 166 (57.8) | 104 (36.2) | 1.753 | 0.7466 |
| | Total Average Score | | | | | | 4.0 | 0.6 |

*Table 2: Fraud Risk Detection in DMBs in Nigeria*

**Mean ≥ 4.0 = 'Satisfied', While **Mean≤ 2.0= 'Dissatisfied'*

*Source: Research Work (2022)*

Table 2 shows that 43.2% of the respondents strongly agreed that there is a whistle blowing mechanism in place to enable employee report identified fraud, 52.6% equally agreed, 1.4% were undecided while 0.3% strongly disagreed. On average, the respondents agreed (M=4.370, SD= 0.631). Similarly, the next item in Table 2 shows that 28.2% of respondents agreed that data analytic procedures are implemented to trigger follow-up investigations of fraudulent transactions, 70% agreed, 1% was undecided while 0.7% disagreed. On average, respondents agreed with a mean = 4.258 and SD = 0.505. Also, Table 2 shows that 48.1% of the respondents strongly agreed that regular reviews of transactions using application controls are conducted to detect fraudulent ones, 51.6% agreed while 0.3% disagreed. Overall the respondent agreed to the question (M= 4.474 and SD = 0.521). Relatedly, 43.6% of the respondents strongly agreed that the internal audit team reviews application controls, investigate all fraud allegations and develops an appropriate work

plan accordingly, while 55.4% agreed and 0.3% were undecided. On average, the respondents agreed (M=4.440, SD= 0.497). On whether the internal audit team performs investigations using applicable professional standards and are free from any conflicts of interest, 61% of the respondents strongly agreed, while 38.7% agreed. This shows that on average, the respondents agreed to the question with a mean = 4.612 and SD = 0.488. Lastly, on the reverse question; whistle blowing mechanism is not in place to enable employees to report identified fraud, 1.4% of the respondents strongly agreed, 2.8% agreed but 1.7% were undecided, 57.8% disagreed while 36.2% strongly disagreed. This means the respondents disagreed with the question with a mean = 1.753 and SD = 0.745. Overall, Table 2 shows that the respondents agreed that information technology control has an effect on fraud risk detection in DMBs in Nigeria. (M= 4.0, SD = 0.6). The analysis above implies that the DMBs also implement fraud risk detection to supplement the fraud risk preventive mechanism where it fails. These detective mechanisms are both human and IT-driven as evidenced from the Table with a huge reliance on Information technology controls. While the Audit team reviews flagged and or suspicious transactions, the IT systems controls can easily flag suspicious transactions based on defined parameters for onward review by the internal control and audit teams. The employment of whistleblowing mechanism, transaction monitoring, data analytics and the other preventive mechanism such as segregation of duties, biometric controls including inbuilt firewall applications, IT processes & controls, fraud risk scoring matrix, reliance on multiple channels of information, specific and industry-wide factors and so on are key variables for attesting to the efficiency of the DMBs Fraud Risk management framework.

*4.2. Regression Tables for Hypothesis*

The Hypothesis was tested using the multiple regression analysis. The data for information technology control (ASC, AAC and NSC) and fraud risk detection 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 | 1.366 | 0.288 | 4.738 | 0.003 |
| ASC | 0.345 | 0.067 | 5.134 | 0.000 |
| AAC | 0.117 | 0.063 | 1.877 | 0.062 |
| NSC | 0.195 | 0.059 | 3.322 | 0.001 |
| $R^2$ | 0.260 | | | |
| Adj $R^2$ | 0.252 | | | |
| S.E of Reg. | 0.209 | | | |
| F-Stat | 30.690 | | | |
| Prob (F-Stat) | 0.000 | | | |
| Df | 265 | | | |

*Table 3: Regression Analysis for Model*
*Dependent Variable: FRD*
*Source: Researcher's Work (2022)*

Note: 5% significance level was adopted
Model

$FRD_i = \beta_0 + \beta_1 ASC_i + \beta_2 AAC_i + \beta_3 NSC_i + e_i$ .....Eq

$FRD_i = 1.366 + 0.345 ASC_i + 0.117 AAC_i + 0.195 NSC_i$

4.2.1. Interpretation

The hypothesis of this study aimed to determine if Information Technology Control has a significant effect on Fraud Risk Detection (FRD) 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 Detection in DMBs in Nigeria. This is represented by the signs of the coefficients $\beta_1, \beta_2$, and $\beta_3$ i.e., $0.345 ASC_i$, $0.117 AAC_i$, and $0.195 NSC_i$ respectively.

This showed that an improvement in the proxies (ASC, AAC and NSC) of the independent variable will lead to an effective fraud risk detection. Also, the value of the constant implies that if the independent variables employed do not exist, FRD would still maintain a positive value of 1.366.

The adjusted $R^2$ value of 25.2% for this model connotes the ability of all the independent variables to collectively explain about 25% variation in Fraud Risk Detection. The remaining 75% 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. The low adjusted $R^2$ of 25.2% was the outcome of the design instrument and the respondents. The instrument was designed with three independent variables to enable the ascertainment of the degree of impact on the respective dependent variables. Responses were indeed aligned to the independent variables and the result further buttresses the fact that the tested independent variables alone cannot significantly explain the variation in Fraud Risk Detection. However, the coefficients further show that the existence of information technology control will contribute positively to fraud risk detection structure.

Furthermore, Table 3 shows the results of regression analysis between information technology control and fraud risk detection. The results on the Table indicates that application security control (ASC) has a significant effect on fraud risk detection in DMBs in Nigeria ($\beta 1 = 0.345$, $t = 5.134$, $p = 0.000 < 0.05$), access/authentication control with ($\beta 2 = 0.117$, $t=1.877$, $p=0.062 < 0.05$), and lastly, network security control with ($\beta 3 = 0.195$, $t = 3.322$, $p = 0.001 < 0.05$). 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 Detection. The F-statistics measures the combined performance of all the independent variables on Fraud Risk Detection. The F-statistics value for this model is 30.69. 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 Detection.

4.2.3. Decision

At the level of significance of 0.05, Degree of Freedom of 3 & 265, F-statistics of 30.69, adjusted $R^2$ of 0.252 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 the model which states that 'Information technology control does not significantly affect Fraud Risk Detection in Deposit Money Banks (DMBs) in Nigeria' is rejected and the alternate hypothesis is accepted with the conclusion that 'Information Technology Control significantly affectFraud Risk Detection in DMBs in Nigeria.'

4.2.4. Discussion of Findings

The finding of the study supports the findings of Okokpujie et al., (2016) who propose the use of data mining techniques that will learn the pattern of customers transactions that can lead to fraud and stop it before it occurs. The study concludes that fraud detection will save the banks from huge losses resulting from fraud if it is nip in the bud. Mousa (2016), Amanze and Onukwugha (2017) also support the use of data mining techniques which is a known application control measure to prevent loan fraud because it is robust enough to detect sophisticated fraud, minimize loss, and scalable to manipulate the large volume of data.

The study also validates an earlier study by Saia et al., (2015) that adopts multiple behavioural models to learn and understand electronic bank users' transaction patterns to detect fraudulent transactions. Similarly, Li et al., (2018) explore the use of the Kernel-Based Supervised Hashing techniques to solve the fraud problem facing e-banking applications. The KSH is a technique used to detect credit card fraud by using past genuine transactions to predict future fraudulent transactions.

Lastly, the study further validates the results of the study carried out by Okonkwo and Ezegbu (2016) and Aladejebi and Oladimeji (2019) where they argued that the traditional internal control mechanism employed by banks have not been adequate in detecting fraud and suggested that banks should create ethics unit and reduce over-reliance on their staff and implement adequate IT control procedures to effectively detect fraud risk since bank transactions are now carried out across the digital platforms.

## 5. Conclusion

From the analysis conducted, it is evident that there is a significant effect of information technology control on fraud risk detection 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 detection.

## 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.

## 7. References


i. ACFE. (2018). Global study on occupational fraud and abuse.
ii. ACFE. (2018). Report to the nations. Asia-Pacific edition.
iii. 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

iv. 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.
v. Ajah, I., &Inyiama, C. (2011). Loan fraud detection and IT-based combat strategies. The Journal of Internet Banking and Commerce, 16(2).
vi. Alao, A. (2016). Forensic auditing and financial fraud in Nigerian deposit money banks (DMBs). European Journal of Accounting, Auditing and Finance Research, 4(8), 1-19.
vii. Albashrawi, M. (2016). Detecting financial fraud using data mining techniques: A decade review from 2004 to 2015. Journal of Data Science, 14(1), 553-570.
viii. Aladejebi, O., &Oladimeji , A. J. (2019). Fraud management among small and medium enterprises in Lagos, Nigeria. The International Journal of Business & Management, 7(3), 227-236.
ix. Alavi, H. (2016). Mitigating the risk of fraud in documentary letters of credit. Journal of European Studies, 6(1), 139-156.
x. Amanze, B. C., &Onukwugha, C. G. (2017). Loan fraud detection system for banking industries in Nigeria using data mining and intelligent agents: The way forward. International Journal of Innovative Research in Technology, Basic and Applied Sciences, 4(1), 1-7.
xi. Ashamu, S. O. (2014). Fraud management in the Nigeria banking industry: Evidence from Nigeria. Journal of Technology, Entrepreneurial and Rural Development, 5(1), 125-137.
xii. 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.
xiii. Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. Financial Innovation, 2(20), 2-10.
xiv. 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.
xv. Chuttur, M. Y. (2013). Overview of the technology acceptance model: Origins, developments and future directions. Indiana University: Working Papers on Information Systems.
xvi. COSO (2016). Fraud risk manageemnt guide. Retrieved December 5, 2021, from https://www.coso.org/documents/coso-fraud-risk-management-guide-executive-summary.pdf
xvii. 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.
xviii. Dubey, R. D., & Manna, A. (2015). E-banking fraud and fraud risk management. Tactful Management Research Journal, 6(1), 20-13.
xix. Desai, N. (2020). Understanding the theoretical underpinnings of corporate fraud. The Journal for Decision Makers, 45(1), 1-7.
xx. 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
xxi. Ezejiofor, R. A., Nwakoby, P. N., &Okoye, J. F. (2016). Impact of forensic accounting on combating fraud in Nigerian banking industry. International Journal of Academic Research in Management and Business, 1(6), 1-19.
xxii. Fadayo, O. M. (2018). An examination of E-banking fraud prevention and detection in Nigeria banks. Unpublished PhD Thesis, De Montfort University. Retrieved June 26, 2021, from https://dora.dmu.ac.uk/bitstream/handle/2086/17520/Oluwalami%20Matthew%20Fadayo%20PhD%20Thesis.pdf?sequence=1&isAllowed=y
xxiii. FITC. (2020). Report on Fraud and Forgery in Nigerian Banks.
xxiv. 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.
xxv. Gangwani, M. (2020). Suitability of forensic accounting in uncovering bank frauds in India: an opinion survey. Journal of Financial Crime, 28(2), 1-16.
xxvi. Georgios, V. L. (2019). Advancing theory of fraud: The S.C.O.R.E. model. Journal of Financial Crime, 26(1), 372-381.
xxvii. 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.
xxviii. 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.
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. 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.

xxxi. 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.

xxxii. Jeyanthi, M. P., Mansurali, A., Harish, V., &Krishnaveni, V. D. (2020). Significance of fraud analytics in Indian banking sectors. Journal of critical reviews, 7(4), 209-213.

xxxiii. 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.

xxxiv. Kariapper, R., Razeeth, S. M., Pirapuraj, P., &Nafrees, A. C. (2020). Effectiveness of ATM and bank security: three factor authentications with systemetic review. Journal of Physics, 1-19.

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

xxxvi. Kolapo, F. T., &Olaniyan, T. O. (2018). The impact of fraud on the performance of deposit money banks in Nigeria. International Journal of Innovative Finance and Economics Research, 6(1), 40-49.

xxxvii. KPMG. (2019). Global banking fraud survey.

xxxviii. Lai, P. (2017). The Literature review of technology adoption models and theories for the novelty technology. Journal of Information Systems and Technology Management, 14(1), 21-38.

xxxix. Li, Z., Liu, G., Wang, S., Xuan, S., & Jiang, C. (2018). Credit card fraud detection via kernel-based supervised hashing. Institute of Electrical and Electronics Engineers Conference, 1249-1254.

xl. Luhach, A. K., Dwivedi, S. K., &Jha, C. K. (2014). Designing and implementing the logical security framework for e-commerce based on service-oriented architecture. International Journal of Advanced Information Technology, 4(3), 25-34.

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

xlii. Madinakhon , K., Dildora , R., Shohsanam , N., &Dilnoza , A. (2019). Banking frauds as a barrier for economic development: Is financial activity under Risky? International Scientific Journal Theoretical & Applied Science, 5(73), 621-629.

xliii. 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.

xliv. Mousa, A. (2016). Detecting financial fraud using data mining techniques: A decade review from 2004 to 2015. Journal of Data Science, 14(1), 553-570.

xlv. 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.

xlvi. 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.

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

xlviii. Ogbonna, K. S., Okaro, C., &Igwe , I. E. (2019). Electronic fraud and credit facilitation of banks in Nigeria. Journal of Accounting Information and Innovation, 5(10), 1-13.

xlix. Ogundana , O., Okere , W., Ogunleye , O., &Oladapo , I. (2018). Forensic accounting and fraud prevention and detection in Nigerian banking industry. COJ Review and Research, 1(1), 1-8.

l. Okokpujie , K. O., John, S. N., Chinyere , K. G., Anele, C., &Olajide, F. (2016). Realtime fraud detection in the banking sector using data mining techniques/algorithms. International Conference on Computational Science and Computational Intelligence, (pp. 1186-1191).

li. Okonkwo, I. V., &Ezegbu, N. L. (2016). Internal control techniques and fraud mitigation in Nigerian banks. Journal of Economics and Finance, 7(5), 37-46.

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

liii. Peters, G. F., Richardson, V. J., & Watson, M. W. (2012). The consequences of Information Technology Control Weaknesses on Management Information Systems: The Case of Sarbanes–Oxley Internal Control Reports. MIS Quarterly, 36(1), 179-203.

liv. 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.

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

lvi. Saia, R., Boratto, L., & Carta, S. (2015). A proactive Time-frame Convolution Vector (TFCV) technique to detect frauds attempts in e-commerce transactions. International Journal of e-Education, e-Business, e-Management and e-Learning, 5(4), 229 -236.

lvii. Uittenbogaard, F. (2015). Introduction seminar: Information and technology audit. The Hague, National Academy for Finance and Economics.
lviii. 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.
lix. Xie, Y., Liu, G., Cao, R., Li, Z., Yan, C., & Jiang, C. (2019). A feature extraction method for credit card fraud detection. 2nd International Conference on Intelligent Autonomous Systems.
lx. Yazici, Y. (2020). Approaches to fraud detection on credit card transactions using artificial intelligence methods. Computer Science & Information Technology, 235-244.
lxi. YuswarZainalBasri, S., &Zulhelmy, T. (2020). S.C.C.O.R.E model to predict the accounting fraud intention. International Journal of Business and Management Invention, 9(10), 28-36.
lxii. Zheng, L., Liu, G., Yan, C., & Jiang, C. (2018). Transaction fraud detection based on total order relation and behaviour diversity. IEEE Transactions on Computational Social Systems, 5(3), 796-806.
lxiii. Zuraidah, S. M., Mohd , F. R., &Yusarina , M. I. (2015). Fraud schemes in the banking institutions: Prevention measures to avoid severe financial loss. Procedia Economics and Finance, 28(1), 107-113.

## Appendix

Questionnaire

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

**Personal Data**

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

| Gender | Department | Academic Qualification |
|---|---|---|
| Male | Internal Audit | Diploma |
| Female | Internal Control | Bachelor degree |
| | Information Technology | Master's degree |
| | | PhD, Post-Doctoral |

*Table 4*

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

**Dependent Variables**

*Fraud Risk Detection in DMBs in Nigeria*

| | Statements | SA | A | U | D | SD |
|---|---|---|---|---|---|---|
| 1 | There is a whistleblowing mechanism in place to enable employees to report identified fraud | | | | | |
| 2 | Data analytic procedures are implemented to trigger follow-up investigations of fraudulent transactions | | | | | |
| 3 | Regular reviews of transactions using application controls are conducted to detect fraudulent ones | | | | | |
| 4 | The internal audit team reviews application controls, investigate all fraud allegations and develops an appropriate work plan accordingly. | | | | | |
| 5 | The internal audit team performs investigations using applicable professional standards and are free from any conflicts of interest | | | | | |
| 6 | A whistleblowing mechanism is not in place to enable employees to report identified fraud | | | | | |

*Table 5*

*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 6*

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 7*

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 8*

[(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;