MANAGING FRAUD IN CONTEMPORARY BUSINESS ENVIRONMENT, THE ROLE OF INFORMATION SECURITY MANAGEMENT: A STUDY OF QUOTED DEPOSIT MONEY BANKS (DMBs) IN NIGERIA

Onajero Kensington OHWO
ORCID: https://orcid.org/0009-0005-7151-4812
Babcock University, Ilesan, Nigeria
Email: ohwo0022@pg.babcock.edu.ng

DOI: 10.52846/MNMK.22.2.06

Abstract:
Every economy relies on the banking sector to boost economic growth and development because of its intermediary role. However, the Nigerian banking sector has been plagued with the risk of fraud which has led to the loss of huge amounts of money annually. This challenge has put pressure on the management of banks on how best to curb the fraud scourge. Although several studies which relied majorly on the traditional method of fraud management have been carried out on how to reduce the frequent occurrence of fraud in the banking sector, the problem persists. Therefore, this study took a different approach to examine the role of information security management on fraud risk management in Deposit Money Banks (DMBs) in Nigeria. The study employed a survey research design. The population of the study was 1,030 staff of the Internal Control, Internal Audit and Information Technology departments of DMBs in Nigeria. A sample size of 288 was determined using Taro Yamane's formula. The respondents were purposively selected from 12 listed banks as at 31st January 2024 due to the role they play in fraud risk management. A structured and validated questionnaire was distributed and 99.7% response rate was achieved. Cronbach's alpha reliability coefficients for the constructs ranged from 0.864 to 0.952. Descriptive and inferential (multiple regression) statistics were used to analyze the data. Utilizing a regression model, the research examines three key proxies of information security management: Application Security Control (ASC), Access/Authentication Control (AAC), and Network Security Control (NSC) and one proxy (Fraud risk governance - FRG) for fraud risk management The model reveals that both ASC and AAC have significant positive effects on FRG, with coefficients of 0.216 and 0.247, respectively, while NSC, with a coefficient of 0.080, does not significantly influence FRG. The model's adjusted R^2 value of 18.9% indicates that these controls collectively explain a modest portion of the variability in FRG, suggesting the presence of other influential factors. The findings highlight that strengthening ASC and AAC can substantially enhance fraud risk governance in Nigerian DMBs, whereas NSC requires further investigation to understand its role. The significance of the overall model, supported by an F-statistic of 21.939 ($p < 0.05$), underscores the importance of integrated information security management in mitigating

fraud risks. Additionally, the study aligns with existing literature advocating for the integration of advanced information security management and traditional fraud management methods. The study recommended that the board of directors of DMBs as part of its oversight function should periodically review the overall fraud risk management framework of the bank to ensure it is current, adequate and effective.

Keywords: information security management, fraud risk governance, fraud risk management.

1. Introduction

The banking sector plays a major role in the development of any economy and it is the catalyst for growth (Nutanix, 2021; Ajala, et al., 2013). This is because the banking system acts as an intermediary between the surplus households that have so much money to save and the deficit households that need money to invest. However, the sector suffers from the occurrence of fraud globally (Desai, 2020; Mukhtaruddin, et al., 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 to take an unjustified advantage of someone (Gangwani 2020; Enofe et al., 2017). Fraud is not limited to Nigeria rather it is a global occurrence (ACFE, 2018) that has led to the failure of multinational companies like Enron, Worldcom, and NITEL (Adetoso & Akinselure, 2016; Olaoye & Dada, 2017).

The remaining part of this study will cover the conceptual review of the main variable, the theoretical framework, the methodology section to show the methods and design followed in this study, the result of the data analysis, the discussion of findings, as well as conclusion and recommendations.

2. Literature Review

2.1 Conceptual Review

This section shows a brief discussion of the main variables (Information security management and fraud management) in this study.

2.1.1 Fraud Risk Management

Fraud risk management is the totality and comprehensive efforts of the management to put the occurrences of fraud near impossible and create strong and effective measures that are capable of preventing or reducing fraud occurrences (Nutanix, 2021; Haoxiang & Smys, 2021). According to Ali (2012), Sang (2014) and Basu (2020) management of every organization must manage its affairs and safeguard its operation from becoming unduly vulnerable to fraudsters and dishonest staff members. Most upper management positions are attached with highly sensitive and classified information, and the top manager's subordinates and supporting staff can be the source of fraud risk, hence adequate security, regular passwords and access models should be changed without notice (Kariapper et al., 2020; Handoko & Tandean, 2021).

Fraud management is the process of assessing and determining fraud-prone areas within an organisation and then efforts made to develop a strong and anti-fraud program that will stop any fraudulent actions before they happen (Rehman & Hashim, 2020; Nutanix, 2021). It involves early identification of possible and inherent fraud risks within and outside the corporation and proactively developing programmes and measures to detect and prevent fraud. The study measures fraud management using fraud risk governance as a proxy.

2.1.2 Information Security Management

Businesses today rely on technology to serve their teaming customers. The Deposit Money Banks (DMBs) over the years have 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 securities and 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, Information security and controls help an organization mitigate the risk involved in the use of technology. These information security and control measures include corporate policies, implementation of security codes, access restrictions, physical security, and automatic edits used in analyzing big data (Richards et al., 2005).

Oniovosa (2015) argued that confidentiality of data transmitted across information systems is paramount as lack of confidentiality can make vital information be accessed by an unauthorized person(s) which could be used to commit fraud. Besides committing fraud with access to unauthorised information, it can cause the organization embarrassment and negatively affect its corporate image thereby portraying a message that the organization is not safe. This will lead to the loss of customers, especially in deposit money banks where the safety of customers' deposits is one of the selling points (Wada & Odulaja, 2012).

Information security management 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 et al., 2012). Information security management is proxied in this study using Application security control, Access control, and Network control.

2.2 Theoretical Review

Theory of Reasoned Action

The theory was conceived by Martin Fishbein and Icek Ajzen in the late 1970s. The theory provides concepts to understand and predict human behaviour. Hagger (2019) identified intention to be the central construct of the theory of reasoned action. He stated that intention mirrors how an individual will likely plan to carry out an event and the effort invested in pursuing a given behaviour. He further conceptualizes intention to be a function of two belief-based constructs viz; attitude and subjective norms with attitude being a positive or negative assessment of accomplishing a particular behaviour in the future, while subjective norms mirror beliefs that third parties would require them to perform a particular behaviour. This means that a person's resolve to act in a particular way is based on the results the person expects will come from acting in that way. Thus, the primary objective of the theory is to understand an individual's behaviour or action by ascertaining the motivation to perform that particular action.

The theory like others has its criticisms. Trafimow (2009) argued that although, the theory of reasoned action has been prominent does not automatically make it a good theory. He stated that one famous criticism of the theory is that it is not falsifiable. He further argued that for a theory to be classified as a good theory it should be falsifiable and since the theory of reasoned action is not falsifiable, then, it is not a good theory irrespective of the number of researchers who believe it to be important.

However, the theory has been used to successfully explain behaviours linked with unethical conduct (Randall, 1989). Sheppard et al., (1988) supported the theory and are of the view that behavioural intentions can be used to predict an involuntary action except the intent changed before performing the action. The reasoned action theory was useful to the study as it helped to determine and predict the behaviour of fraudsters to ascertain the best information security management control to implement to detect and prevent the occurrence. It also unravelled and helped to understand the intentions of the fraudsters and why they want to commit fraud thereby making it easy to implement the right information security control. This is because knowing the intention of the fraudster will help determine the best controls to implement since there is no universal control that works for all fraud intents (Hagger, 2019).

2.3 Empirical Review

Banks have applied information security management controls to prevent fraud and make the e-banking platforms more appealing to customers. Diadiushkin et al., (2019) conducted a study that focused on fraud discovery and the ways to fully automate the process. The study lends support to the use of machine learning algorithms in fraud risk governance in instant payments and proposes the use of artificial intelligence like Random Forest or Bank Sealer. Abdulrahman (2019), and Ivashkovskaya and Ivaninskiy (2020) also supported the use of artificial intelligence in fraud risk governance but Lutui and Ahokovi (2017) and Sadgali et al., (2019) disagreed on the sole use of information security controls in the governance of fraud risk and advocate the implementation of hybrid fraud risk governance techniques because they combine and harness the benefits of several traditional governance methods with artificial intelligence techniques.

However, Yazici (2020) opined that the use of artificial intelligence may not be effective in fraud risk governance. The study identified the challenges of using artificial intelligence to include the imbalanced data set, real-time working scenarios, and feature engineering and concluded that it will take some time to achieve online real-time fraud risk governance using artificial intelligence because of the inherent challenges facing the technology. Similarly, Bahnsen et al., (2013) fault the current use of machine learning algorithms that did not consider the real cost of credit card fraud as a means to evaluate the algorithm. Thus, the paper proposes the usage of comparison measures that realistically represent the financial gains and losses occasioned by fraud risk governance.

Siddiqui and Ahmad (2013) and Shewangu (2014) while examining the role of technology in fraud risk governance found that proper implementation of advanced information technology system application, training and alignment with the corporate objective help in implementing effective fraud risk governance in the banking system.

Although Emad and Salam (2015) and Haoxiang and Smys (2021) propose the use of the transaction tracking' model to help the Board and management in the fraud governance process, Shaikh and Shah (2012) and Juhandi et al., (2020)

recommend the implementation of real-time information security control that can prevent and detect fraud at the ATM terminal thereby improving fraud risk governance because Shaikh and Shah (2012) found that a total collapse of the control in ACB bank led to the ATM fraud where 2,430 fraudulent transactions worth 21 million Pakistan currency was conducted using 228 ATM cards for 89 consecutive days before it was detected. Therefore to enhance fraud risk governance in real-time, Abbasi et al., (2012), and Amanze and Onukwugha (2018) propose the use of intelligent agents and data mining techniques, while, Qiu and Li (2017) advocate designing a trusted tracking system that can incorporate incident tracking, data exploration, risk analysis, and security alerts into the application for real-time fraud risk governance. But Demiriz and Ekizoglu (2016) discovered that many ATM users do not leave their vicinity making it easier to detect fraud committed using their debit cards in other vicinities. This is made possible by using a unique approach to detect fraudulent patterns from Automated Teller Machine (ATM) using data by evaluating geo-behavioural patterns of the customers and classifying financial transactions into suspicious and non-suspicious using a fuzzy rule-based system. This means fraudulent transactions could easily be identified and prevented in real-time giving management an overall view of activities thereby improving the governance over fraud risk.

Relatedly, Bhasin (2016) in his study of the role of technology in combating fraud discovered that banks can leverage the use of advanced technology and analytics in building a robust governance structure that will help reduce fraud loss and this assertion was supported by Grove et al., (2018). In addition, Vincent et al., (2010), Madhavi and Sahoo (2016) and Ahmad and Alam (2016) opined that the advanced technology to implement to aid fraud risk governance in real-time is biometric using Elliptic Curve Cryptography (ECC) which requires lesser key size (between 224-255 key size) and inbuilt security of OTP using palm-vein as the biometric security apparatus. This is because of the security flaws associated with the majority of the OTPs being used that require large key sizes for encryption (e.g RSA algorithm requires 2048 bits key size for it to achieve 112 bits security level); the storage of keys in the application which can easily be compromised using brute force attack. Nevertheless, Muntjir and Siddiqui (2013) opposed using only one specific technology in enhancing fraud risk governance and advocate the use of traditional control infused with biometric security features to improve risk governance and make e-banking channels more secure for customers and promote confidence in e-banking. However, Enofe et al., (2017) and Idogei et al., (2017) advocated the sole use of strong internal control and traditional governance measures in managing fraud risk.

Using a more dynamic technology to promote fraud risk governance in real-time, Rahmana and Anwar (2014) opined that proper appraisal of software or application is the most effective means of enhancing fraud risk governance in banks but Onyesolu and Okpala (2017), Kariapper et al., (2020) although align with Rahmana and Anwar's position discovered that the implementation of 3-factor authentication method helps in promoting fraud risk governance. Nevertheless, Sabani and Rishan (2019) argue that a two-factor verification method with a PIN and biometric or secure code with One-Time-Password is more effective in fraud risk governance than any other method. However, Kogan and Kim (2014) conducted a study where they proposed a multi-step fraud risk governance model that analyses transactions at different levels and isolates suspected fraudulent ones. The study

simulated transactions using the model and was able to identify drawbacks to the successful implementation of the model.

Although Adetiloye et al., (2016) confirm that information security control can be used to reduce cash handling thereby reducing ATM fraud, the study however posited that paying handsome remuneration to bank employees will reduce fraud and enshrine an effective fraud risk governance structure, thus, banks should review the salaries of their employees from time to time.

3. Research objectives

Since the persistent occurrence of fraud has a negative impact on the DMBs, the main objective of this study, therefore, is to examine the impact of information security management on fraud management in quoted DMBs in Nigeria. To achieve the main objective of this study, the following specific objective was set: to determine the influence of information security management on fraud risk management in quoted DMBs in Nigeria;

3.1 Methodology of research

Since the study focused on determining the role of information security management in managing fraud, opinions and vital facts from bankers who are central to the fraud scourge ravaging the banks were essential to the study. Consequently, the survey research design was adopted in the study because it provided an accurate method of evaluating the characteristic features of the entire population through a carefully selected sample drawn from the defined population in a relatively quick manner (Hyman & Sierra, 2016). The primary data to be used for this study was extracted from the copies of the questionnaire administered to selected bank officials who are knowledgeable about information security control and fraud management in the DMBs in Nigeria.

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.

$n = 1030/\{1 + 1030\ (0.05)^{2}\}$

$n = 1030/.4$

$n = 288$

The research instrument used in this study is a 5-Point-Likert-scale questionnaire targeted at determining the effect of information security management in curbing fraud in DMBs in Nigeria. The 5-point Likert scale was chosen for the study because it is easy to understand thereby increasing the response rate as well as the quality of response (Keith, 2018).

To ensure the validity of the research instrument (the questionnaire), there was an extensive literature review relating to the topic which satisfied theoretical validity. However, to further examine the evidence of content validity, the instrument was initially reviewed by a professional banker who is a member of management and an expert in managing fraud in the bank to ensure the content validity of the research instrument. Reliability of the research instrument was conducted using Cronbach's Alpha method as shown below:

Table 1. Reliability Test

SN	Construct	No of Items	Cronbach's Alpha
1	Fraud Risk Governance (FRG)	5	0.952
2	Application Security Control (ASC)	5	0.864
3	Access/Authentication Control (AAC)	5	0.926
4	Network Security Control (NSC)	5	0.934

Source: Researcher's Computation, 2024

The model that was used in ascertaining the effects of the independent variables on the dependent variables of the study is specified in this section as:

$Y=f(X)$
Where
$Y = y_1, y_2, y_3, y_4, y_5$
$X = x_1, x_2, x_3$
Functional Relationship
FRG = *f*(ASC, AAC, NSC) …….(eqn.1)
Regression Models
Model
$FRG_i = \beta_0 + \beta_1 ASCi + \beta_2 AACi + \beta_3 NSCi + e_i$
Where:
$ß_0$ = Intercept u=R residual
e= Error Term
i = Cross-sectional Variable
FRG = Fraud Risk Governance
ASC = Application security control
AAS = Access/Authentication control
NSC = Network security control

3.2 Research question.

To meet the specific objectives, research question was framed with the aim of the question being answered in this study. The research question is: how does information security management influence fraud risk management in quoted DMBs in Nigeria?

4. Results and discussion

4.1 Analysis of Respondents Response

Table 2. Fraud Risk Governance in DMBs in Nigeria

	Statements	SA	A	U	D	SD	Mean	Std. Dev.
1	The Board of directors are responsible for ensuring that management designs effective fraud risk management process using information security controls.	127 (44.3)	159 (55.4)	0 (0.0)	1 (0.3)	0 (0.0)	4.435	0.517
2	The Board of directors maintains oversight of the fraud risk management framework using information security controls.	83 (28.9)	202 (70.4)	0 (0.0)	1 (0.3)	1 (0.3)	4.272	0.511
3	The board of directors ensures that the internal audit department has unrestricted access to the board or a committee of the board (audit committee)	148 (51.6)	139 (48.4)	0 (0.0)	0 (0.0)	0 (0.0)	4.516	0.501
4	Management has designed an effective fraud management framework including policies and information security control procedures.	125 (943.6)	161 (56.1)	0 (0.0)	0 (0.0)	0 (0.0)	4.437	0.497
5	The board monitors the effectiveness of the fraud risk management program through data analytics mechanism and addresses the topic quarterly as an agenda item during board meetings	159 (55.4)	125 (43.6)	0 (0.0)	1 (0.3)	0 (0.0)	4.551	0.519
6	The Board of directors are responsible for ensuring that management designs effective fraud risk management process using information security controls.	4 (1.4)	3 (1.0)	0 (0.0)	161 (56.1)	119 (41.5)	1.648	0.678
	Total Average Score						**4.0**	**0.6**

**Mean ≥ 4.0 = "Satisfied", While **Mean≤ 2.0= "Dissatisfied"*
Source: Research Work (2024)

Table 2 shows that 44.3% of the respondents strongly agreed that the Board of Directors are responsible for ensuring that management designs effective fraud risk management policies that encourage ethical behaviour, 55.4% equally agreed while 1% disagreed. On average, the respondents agreed (M=4.435, SD= 0.517). Similarly, the next item in Table 2 showed that 28.9% of respondents agreed that the board of directors maintains oversight of the fraud risk management framework using information security controls, 70.4% agreed, 0.3% were undecided and 0.3% disagreed. On average, respondents agreed that the board of directors maintains oversight of the fraud risk management framework using information security controls with an average mean of 4272 and SD of 0.511. Also, Table 2 showed that 51.6% of the respondents strongly agreed that the Board of Directors ensure that the internal audit department has unrestricted access to the board or a committee of the board (audit committee) while 48.4% agreed. Overall the respondent agreed with the question (M= 4.516 and SD = 0.501). Relatedly, 43.7% of the respondents strongly agreed that Management has designed an effective fraud management framework including policies and procedures, while 56.3% agreed. On average, the respondents agreed (M=4.437, SD= 0.497).

On whether the board monitors the effectiveness of the fraud management program and addresses the topic quarterly as an agenda item during board meetings, 55.43% of the respondents strongly agreed, 43.6% agreed, and 0.3% disagreed. This showed that on average, the respondents agreed with the question with a mean = 4.551 and SD = 0.519. Lastly, on the reverse question; the Board of Directors are not responsible for ensuring that management designs effective fraud risk management policies that encourage ethical behaviour, 1.4% of the respondents strongly agreed, 1% agreed but 56.1% disagreed and 41.5% strongly disagreed. This means that the respondents disagreed with the question with a mean = 1.648 and SD = 0.678.

Overall, Table 2 shows that the respondents agreed that information security management affects fraud risk governance in DMBs in Nigeria. (M= 4.0, SD = 0.6). The analysis, therefore, implies that there is a fraud risk governance among DMBs and duly acknowledged by their respective board of directors including senior management. Accountabilities and responsibilities for fraud risk governance are known and delineated between Board and Senior Management. This however has a positive impact on fraud management.

4.2 Regression Tables for Hypothesis

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

Table 3. Regression Analysis for Model

MODEL				
Variable	Coeff	Std. Err	T-Stat	Prob
Constant	1.812	0.271	6.677	0.000
ASC	0.216	0.064	3.380	0.001
AAC	0.247	0.059	4.165	0.000
NSC	0.080	0.056	1.434	0.153
R^2	0.198			
Adj R^2	0.189			
S.E of Reg.	0.199			
F-Stat	21.939			
Prob (F-Stat)	0.000			
Df	269			

Dependent Variable: FRG
Source: Researcher's Work (2024)
Note: 5% significance level was adopted

Model 1

$FRG_i = \beta_0 + \beta_1 ASCi + \beta_2 AACi + \beta_3 NSCi + e_i$

$FRG_i = 1.812 + 0.216ASC_i + 0.247AAC_i + 0.080NSC_i$

4.3 Interpretation

Hypothesis two of this study aimed to determine if Information Security Management Control has a significant effect on Fraud Risk Governance (FRG) 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 (ASC), Access/Authentication control (AAC), and Network Security Control (NSC)) and Fraud Risk Governance in DMBs in Nigeria. This is represented by the signs of the coefficients β_1, β_2, and β_3 i.e., $0.216ASC_i$, $0.247AAC_i$, and $0.080NSC_i$ respectively.

This shows that an improvement in the proxies (ASC, AAC and NSC) of the independent variable will lead to good fraud risk governance. Also, the value of the constant implies that if the independent variables employed do not exist, FRG would still maintain a positive value of 1.812.

The adjusted R^2 value of 18.9% for this model connotes the ability of all the independent variables to collectively explain about 19% variation in Fraud Risk Governance. The remaining 81% 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 for the model. The low adjusted R^2 of 19% was the outcome of the design instrument. 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 Governance. However, the coefficients further

showed that the existence of information security management control will contribute positively to the fraud risk governance structure.

Furthermore, Table 3 shows the results of regression analysis between information security management control and fraud risk governance. The results in the Table indicated that application security control (ASC) has a significant effect on fraud risk governance in DMBs in Nigeria (β1 = 0.216, t = 3.380, p= 0.001< 0.05), access/authentication control with (β2 = 0.247, t=4.165, p=0.000 < 0.05), and lastly, network security control with (β3= 0.080, t= 1.434, p= 0.153 < 0.05). The t-statistics reflect the individual significance of the variables in this model. It showed that all the proxies of the independent variable (Application security control (ASC), Access/Authentication control (AAC), and Network Security Control (NSC) had a significant relationship with Fraud Risk Governance. The F-statistics measures the combined performance of all the independent variables on Fraud Risk Governance. The F-statistics value for this model is 21.939. 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 showed that the combined proxies of Information Technology Management have a significant effect on Fraud Risk Governance.

Decision

At the level of significance = 0.05, df = 3, 269, F-statistics = 21.939, adjusted R^2 = 0.189 and p-value = 0.0000 which is less than the 0.05 level of significance adopted for the study, the null hypothesis for model two which stated that "Information technology management does not significantly affect Fraud management in Deposit Money Banks (DMBs) in Nigeria" was rejected. Thus, the alternate hypothesis was accepted with the conclusion that "Information Security Management significantly affect Fraud Management in DMBs in Nigeria.".

Discussion of Findings

The findings of the study substantiate the findings of Diadiushkin et al., (2019), Ivashkovskaya and Ivaninskiy (2020) and Flowerastia et al (2021). The studies focused on fraud discovery and the ways to fully automate the fraud risk governance process. The studies lend support to the use of machine learning algorithms in fraud risk governance in instant payments and propose the use of artificial intelligence like Random Forest or Bank sealer. Abdulrahman (2019) also support the use of artificial intelligence in fraud risk governance but Sadgali et al., (2019) disagreed with the sole use of information security management controls in the governance of fraud risk and advocated the implementation of hybrid fraud risk governance techniques because they combine and harness the benefits of several traditional governance methods with artificial intelligence techniques.

Since adequate fraud risk governance will reduce incidents of fraud and save the bank attendant cost occasioned by fraud loss, this study further validated the findings of Bahnsen et al., (2013) that faulted the use of machine learning algorithms that did not consider the real cost of credit card fraud as a means to evaluating the algorithm. Thus, the paper proposes the usage of comparison measures that realistically represent the financial gains and losses occasioned by fraud risk governance.

Lastly, the findings of this study showing that the board and management monitor the fraud risk governance process further validated the finding of Emad and Salam (2015) and Haoxiang and Smys (2021) who proposed the use of the 'transaction tracking' model to help the Board and management in the fraud risk governance monitoring process. Therefore to enhance fraud risk governance in real-

time, Abbasi et al., (2012), and Amanze and Onukwugha (2018) propose the use of intelligent agents and data mining techniques, while, Qiu and Li (2017) advocate designing a trusted tracking system that can incorporate incident tracking, data exploration, risk analysis, and security alerts into the application for real-time fraud risk governance.

This study however supported the referenced studies because the corporate governance process is the same across the globe and is highly regulated by the government and global regulatory standards. However, the implication of the findings of the study means that with well-implemented information security management, the fraud risk governance process in the deposit money banks in Nigeria will improve. The board of directors in conjunction with the bank's management will have a holistic view of the fraud risk management process; how adequate it is, inherent gaps in the process and put measures in place to strengthen the process to make it more effective. The implication is that with effective information security management and improved fraud risk governance process, incidents of fraud in the banks will be reduced and more customer patronage will be recorded with an attendant positive impact on the bank's annual financial performances. It will also accord the board of directors of the banks the opportunity to understand the dynamics of the fraud risk inherent in the banking sector and prepare them to carry out the required oversight function effectively.

5. Conclusions

From the analysis conducted, the following conclusions were made:

There is a significant effect of information security management on fraud risk management in DMBs in Nigeria with regard to fraud risk governance. 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 obtained in the analysis affirmed the conclusion that information security management has a significant effect on fraud risk governance.

Information security management has a significant effect on fraud risk governance in DMBs in Nigeria. Given the p-value of 0.000 for fraud risk governance that is less than the level of significance of 0.05 adopted by the study, it can therefore be concluded that information security management has a significant effect on fraud risk management.

6. Recommendation

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

The Managing Directors/CEOs of DMBs should review and develop a hybrid model that leverages both automated systems and human oversight to enhance the effectiveness of fraud risk management.

Also, the Board of Directors of DMBs saddled with governance responsibilities should place more emphasis on fraud risk management and the level of information security management controls that have been implemented to enhance the fraud risk governance process in the banks.

The Managing Directors/CEOs of the DMBs should give priority to the implementation of information security management control across all their digital channels or platforms as this will help to prevent the risk of fraud on the platforms.

The Managing Directors/CEOs of deposit money banks should put measures in place that will ensure periodic reviews of the adequacy of the implemented information security management controls and fraud governance medium to ensure that they remain effective and work as designed. Also, since technology is evolving, the information securities built into digital platforms or applications should be reviewed and monitored to ensure that they align with the technological changes.

The board of directors of DMBs as part of her oversight function should periodically review the overall fraud risk management framework of the bank to ensure it is current, adequate and effective. Also, the staff in the departments responsible for managing fraud risk should be adequately trained and equipped with the requisite skills in using information security tools to manage fraud.

REFERENCES

Abbasi, A., Albrecht, C., Vance, A., & Hansen, J. 2012. Metafraud: A meta-learning framework for detecting financial fraud. *MIS Quarterly, 36*(4), 1293-1327. https://doi.org/10.2307/41703508

Abdulrahman, M. H. 2019. The impact of Artificial Intelligence (AI) in detecting fraud in the UAE. *Electronic Interdisciplinary Miscellaneous Journal, 10*(1), 3-19.

ACFE. 2018. *Global study on occupational fraud and abuse.*

ACFE. 2018. *Report to the nations. Asia-Pacific edition.*

Adetiloye, A. K., Olokoyo, O. F., & Taiwo, N. J. 2016. Fraud prevention and internal control in the Nigerian banking system. *International Journal of Economics and Financial Issues, 6*(3), 1172-1179.

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.

Ahmad, K., & Alam, M. S. 2016. E-Commerce security through elliptic curve cryptography. *Procedia Computer Science, 78*(1), 867-873. https://doi.org/10.1016/j.procs.2016.05.549

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

Ali, H. 2012. An analysis of identity theft: Motives, related frauds, techniques and prevention. *Journal of Law and Conflict Resolution, 4*(1), 1-12. 10.5897/JLCR11.044

Amanze , B. C., & Onukwugha, C. G. 2018. Data mining application in credit card fraud detection system. *International Journal of Trend in Research and Development, 5*(4), 23-26.

Bahnsen, A. C., Stojanovic, A., Aouada, D., & Ottersten, B. 2013. Cost-sensitive credit card fraud detection using Bayes minimum risk. *12th International Conference on Machine Learning and Applications, Miami*. 10.1109/ICMLA.2013.68

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.

Bhasin, M. L. 2016. The role of technology in combatting bank frauds: perspectives and prospects. *Ecoforum, 5*(2), 200-212.

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. 10.4018/joeuc.2012040103

Demiriz, A., & Ekizoglu, B. 2016. Fuzzy rule-based analysis of spatio-temporal ATM usage data for fraud detection and prevention. *Journal of Intelligent & Fuzzy Systems*, 805–813. 10.3233/JIFS-169012

Desai, N. 2020. Understanding the theoretical underpinnings of corporate fraud. *The Journal for Decision Makers, 45*(1), 1-7. https://doi.org/10.1177/0256090920917789

Diadiushkin, A., Sandkuhl, K., & Maiatin, A. 2019. Fraud detection in payments transactions: Overview of existing approaches and usage for instant payments. *Complex Systems Informatics and Modeling Quarterly, 118*(20), 72–88. https://doi.org/10.7250/csimq.2019-20.04

Emad, A.-S., & Salam, M. 2015. Security and fraud issues of e-banking. *International Journal of Computer Networks and Applications, 2*(4), 179-187.

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. Abstract 10.6007/IJARBSS/v7-i7/2021

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. 10.2991/assehr.k.210805.038

Gangwani, M. 2020. Suitability of forensic accounting in uncovering bank frauds in India: an opinion survey. *Journal of Financial Crime, 28*(2), 1-16. https://doi.org/10.1108/JFC-07-2020-0126

Grove, H., Clouse, M., & Schaffner, G. L. 2018. Digitalization impacts on corporate governance. *Journal of Governance and Regulation, 7*(4), 51-63. 10.22495/jgr_v7_i4_p6

Hagger, M. S. 2019. The reasoned action approach and the theories of reasoned action and planned behaviour. In D. S. Dunn (Ed.), *Oxford Bibliographies in Psychology.* New York, NY: Oxford University Press. 10.1093/OBO/9780199828340-0240

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. 10.36548/jeea.2021.1.001

Hyman, M. R., & Sierra, J. J. 2016. Open- versus closed-ended survey questions. *New Mexico State Unversity: Business Outlook, 14*(2), 1-5.

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.

Ivashkovskaya, I., & Ivaninskiy, I. 2020. What impact does artificial intelligence have on corporate governance? *Journal of Corporate Finance Research, 14*(4), 90-101. https://doi.org/10.17323/j.jcfr.2073-0438.14.4.2020.90-101

Juhandi, N., Zuhri1, S., Fahlevi, M., Noviantoro , R., Nurabdi, M., & Setiadi. 2020. Information technology and corporate governance in fraud prevention. *Web of Conferences*, 2-10. https://doi.org/10.1051/e3sconf/202020216003

Kariapper, R., Razeeth, S. M., Pirapuraj, P., & Nafrees, A. C. 2020. Effectiveness of ATM and bank security: three-factor authentications with systematic review. *Journal of Physics*, 1-19. 10.1088/1742-6596/1712/1/012007

Keith, T. S. 2018. The use of Cronbach's Alpha when developing and reporting research instruments in science education. *Research Science Education, 48*(1), 1273–1296. 10.1007/s11165-016-9602-2

Kogan, A., & Kim, Y. 2014. Development of an anomaly detection model for a bank's transitory account system. *Journal of Information Systems, 28*(1), 145-165. https://doi.org/10.1108/978-1-78743-085-320191009

Lutui, R., & Ahokovi, T. 2017. Financial fraud risk management and corporate governance. *Australian Information Security Management Conference*, 5-13. 10.4225/75/5a84f10795b47

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

Madhavi, K., & Sahoo, P. K. 2016. OTP using biometrics embellish security for Online – Transactions (OLT). *International Journal of Advance Computing Technique and Applications, 4*(1), 220-226.

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. https://doi.org/10.15739/IBME.20.002

Muntjir, M., & Siddiqui, A. T. 2013. A study of possible biometric solution to curb frauds in ATM transaction. *IJASCSE, 2*(3), 1-6.

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

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. http://dx.doi.org/10.19044/esj.2017.v13n31p290

Oniovosa, O.E. 2015. Application of firewall security to internet security. *International Journal of Information Technology and Business Management, 15*(1), 64-71.

Onyesolu , M. O., & Okpala, A. C. 2017. Improving security using a three-tier authentication for automated teller machines. *I. J. Computer Network and Information Security, 10*(1), 50-56. 10.5815/ijcnis.2017.10.06

Owolabi, A. S. 2010. Fraud and fraudulent practices in Nigeria banking industry. *African Research Review, 4*(3), 240-256. 10.4314/afrrev.v4i3.60263

Qiu, L., & Li, J. 2017. Covering the monitoring network: A unified framework to protect e-commerce security. *Hindawi Complexity*, 1-11. https://doi.org/10.1155/2017/6254842

Rahmana, R. A., & Anwar, I. S. 2014. Effectiveness of fraud prevention and detection techniques in Malaysian Islamic banks. *Procedia - Social and Behavioral Sciences*, 97 – 102. https://doi.org/10.1016/j.sbspro.2014.06.015

Randall, D. M. 1989. Taking stock: Can the theory of reasoned action explain unethical conduct. *Journal of Business Ethics, 8*(11), 873-882.

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. https://doi.org/10.2478/bsrj-2020-0002

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

Sabani, M. J., & Rishan , U. M. 2019. Effectiveness of ATM security mechanisms: A review analysis. *Proceedings of 9th International Symposium, South Eastern University of Sri Lanka*, 234-243. http://ir.lib.seu.ac.lk/handle/123456789/3927

Sadgali, I., Sael, N., & Benabbou, F. 2019. Performance of machine learning techniques in the detection of financial frauds. *Procedia Computer Science, 148*(1), 45–54. https://doi.org/10.1016/j.procs.2019.01.007

Sang, J. M. 2014. Determinants of fraud control measures in commercial banks: A survey of selected commercial banks in Nakuru town, Kenya. *International Journal of Science and Research, 3*(10), 2178-2183.

Shaikh, A. A., & Shah, S. M. 2012. Auto Teller Machine (ATM) fraud – case study of a commercial bank in Pakistan. *International Journal of Business and Management, 7*(22), 100-108.

Sheppard, B. H., Hartwick, J., & Warshaw, P. R. 1988. The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *Journal of Consumer Research, 15*(3), 325–343. https://doi.org/10.1086/209170

Shewangu, D. 2014. Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. *Risk governance & control: financial markets & institutions, 4*(2), 18-26.

Siddiqui, A., & Ahmad, N. 2013. Fraud risk – The role of information technology. *IJMS, 1*(1), 48-52.

Trafimow, D. 2009. The theory of reasoned action: A case study of falsification in psychology. *Theory of Psychology, 19*(4), 501-518. https://doi.org/10.1177/0959354309336319

Vincent, O. R., Folorunso, O., & Akinde, A. D. 2010. Improving e-payment security using Elliptic Curve Cryptosystem. *Electronic Commerce Research, 10*(1), 27-41.

Wada, F., & Odulaja, O. G. 2012. Electronic banking and cybercrime In Nigeria - A theoretical policy perspective on causation. *African Journal of Computing & ICT, 5*(1), 69-82.

Yazici, Y. 2020. Approaches to fraud detection on credit card transactions using artificial intelligence methods. *Computer Science & Information Technology*, 235-244. https://doi.org/10.48550/arXiv.2007.14622