



## The analysis of drivers of operational risks in Nigerian commercial banks

 Olajide Solomon Fadun<sup>(a)</sup>  Diekolola Oye<sup>(b)</sup>



<sup>(a,b)</sup> Department of Actuarial Science and Insurance, University of Lagos, Lagos, Nigeria.

### ARTICLE INFO

#### Article history:

Received 12 October 2021

Received in rev. form 21 Nov. 2021

Accepted 08 December 2020

#### Keywords:

Operational risk, operational loss, internal process, quality of risk officers, IT systems

#### JEL Classification:

G21, G32

### ABSTRACT

*Despite the institutionalization of operational risk management in banks and the strict supervision of bank regulators, operational risk events are still on the increase. It is becoming evident to banks that there is a need to identify the drivers of this risk and nib it at the root to reduce the probability of recurrence. Hence, this study examined the drivers of operational risks in Nigerian commercial banks and the extent to which each driver contributes to operational risk. To achieve the study's objectives, primary data were collected from the Operational Risk Management Desks of six (6) sampled commercial banks and analysed using SPSS and Microsoft Excel. The result showed that Internal Process, IT system and Quality of Risk Officers are determinants of operational losses in banks. Internal process was however indicated as having the most impact. The study concluded that Internal Process is the major driver of operational risk in Nigerian Commercial banks. The researcher therefore recommends that bank management must have defined procedures for core activities and prioritize regular review of their critical processes to reduce operational risk events and the associated costs.*

© 2021 by the authors. Licensee Bussecon International, Istanbul, Turkey. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International license (CC BY) (<http://creativecommons.org/licenses/by/4.0/>).

## Introduction

In prior decades, banks had focused more on the traditional credit risk and market risk areas. The narrative however changed after the worldwide collapse of large banks and the 2008 financial crisis which were alleged to have been caused by inadequate operational risk management (Tandon & Mehra, 2017). The failures spurred several discussions amongst the regulators which led to the institutionalization of operational risk management in financial institutions. However, in recent years, data from public sources and various risk media publications suggest that operational risks are not effectively managed in financial institutions; surprising is the fact that this includes banks that are presumed to have robust risk management systems. For instance, major operational losses of \$175.5m and \$22m were recorded by Bank of America and Citigroup respectively in 2012 as well as \$1b and €252m by Rabobank and Fondiaria-SIA in 2013 (Pakhchanyan, 2016). Public data also indicated huge operational losses spanning from the £8.2m and \$187.5m penalties paid by Aviva and Wells Fargo respectively in 2016 for failure to maintain adequate internal controls and manage their operational risks; \$880m fraud loss of Catalunya Caixa (a Spanish bank) in 2017; and the \$5.5b and \$2.2b fraud losses in PrivatBank and Punjab National Bank in 2019 (Risk Net, 2018; Risk Net, 2019). These losses ultimately have both financial and non-financial implications on banks. Though several investigations had been conducted which established the impact of operational risk on the performance of banks including studies done by Bekele (2015), Muriithi (2016), Ng'aari (2016), Simamora and Oswari (2019), Fadun and Oye (2020), there are however few examining the main drivers of this risk. Ordinarily, one would have expected that factors such as; availability of historical information on operational loss events, proliferation of operational risk management practices and the stiff penalties imposed for not complying with applicable regulatory directives would have reduced the frequency

\* Corresponding author. ORCID ID: 0000-0003-0882-6248

© 2021 by the authors. Hosting by Bussecon International Academy. Peer review under responsibility of Bussecon International Academy.

<http://dx.doi.org/10.36096/brss.v3i3.293>

Citation: Fadun, O. S., & Oye, D. (2021). The analysis of drivers of operational risks in Nigerian commercial banks. *Bussecon Review of Social Sciences* (2687-2285), 3(3). <https://doi.org/10.36096/brss.v3i3.293>

at which large operational risk events crystallizes, current realities however it indicates otherwise. This suggests that banks may not have in-depth knowledge about the drivers leading to operational loss. According to Chua's 1996 study (as cited in Hemrit & Arab, 2013), identifying the main drivers of operational risk event is vital as it can assist an organisation have better understanding of its risk exposures which will elicit adequate measures necessary to mitigate the risks.

This study, therefore, examined drivers of operational risks in Nigerian commercial banks and the extent to which each driver contributes to operational risk. Due to time and cost constraints, six (6) (out of the 20 licensed commercial banks in Nigeria at the time of this study) were considered in this study. To achieve the objective of the study, questionnaires were administered to the operational risk management officers of the selected banks to collect primary data on operational risk drivers including internal process, system and quality of risk officers and how these drivers impact on operational loss. Some of these officers were also interviewed to gain better insights into how the drivers contribute to operational loss. Based on the results of the data analysis, the study concluded that Internal Process, IT system and Quality of Risk Officers are critical sources of operational loss in banks, however, internal process was determined to be the driver with the most impact.

The remaining part of this paper focused on literature review, empirical review, hypothesis development, methodology, data collection instrument, ethical issues, findings, hypothesis testing, discussion and conclusion.

## **Literature Review**

Sources of operational risk can either be internal or external to the business and are often generated by processes, technology and people (CIMA, 2008). Internal sources may include inadequate internal process development, poor system and unprepared staff. On the other hand, external sources may include state of the economy, high rate of innovation in the technological and telecommunication environment (Radu & Olteanu, 2009). Kamau's 2010 study (as cited in Siminyu, Clive & Musiega, 2017) suggested that operational risk in banks is largely driven by automated technology, quality of staff, management support and frauds. This was corroborated by Sultania (2018) who asserted that the main sources of operational risks are human error, IT failures and failures of internal processes to accurately transmit information. Hemrit and Arab (2013) study also asserted that potential sources of operational risk may be shortages of skilled staff as well as inadequate process documentation and implementation which may lead to huge losses. The study emphasized the need to involve the operators in identifying and managing their risks and have experienced risk officers with the right skills for effective identification of potential operational risks in the face of increasing rapid changes in the environmental, business and technological space. Abdullah, Farouk and Bassam (2018) asserted that people risk constitute a major source of operational risk which may manifest in form of high workload for employees, inadequately trained employees and high staff attrition without corresponding replacements. However, according to BCBS (2011), internal processes, people, systems or external events are highlighted as the main drivers of operational risks in financial institutions.

A consensus among many of the researchers seemed to be that there is a strong relationship between quality of people and effective management of risk. This notion was also resounded by Accenture (2015) who asserted that practical experience and training combined with an improved understanding of the business processes, procedures and products will help operational risk management functions to accurately identify risk, assess risks and ultimately impact positively on returns. This view was also corroborated by BCBS (2014) which highlighted that the operational risk function must be adequately staffed with personnel that possesses the requisite skills necessary for the effective management of risks.

Staff is one of the major contributors to operational losses. Staff can erroneously or intentionally cause huge losses when they do not adhere to stipulated policies, standards and procedures. Unintentional errors mainly stem from knowledge gaps, work-overload and unclear policies/procedures which may lead to sloppy execution of deliverables. Compromised staff can also carry out intentional breaches e.g., unauthorized transactions, which also leads to huge direct operational losses as well as legal and regulatory costs (Bains & Company, 2018). People risk is especially high for retail banks (i.e. mass-market banking or consumer banking that provide banking services to the public, rather than to companies, corporations or other banks) because these banks usually have large staff strength that process high volume of transactions. Many of these staff are also overworked due to the high number of mundane transaction requests treated daily. More so, due to the pressure of work, many of these staff are not exposed to sufficient trainings which also inadvertently increases the error rates (Abdullah, Farouk & Bassam, 2018; Knezevic, 2013). Increase in staff workload can also predispose them to higher error rates which translates to higher operational losses and vice versa. For example, the research conducted by Xu, Tan and Netessine (2017) on the impact of workload on operational losses on a commercial bank in China showed that optimal staffing would decrease the number of operational risk events by 4.51%, reduce total losses by 4.58% and increase profits by 1.24%. The culture and strategy of an organization may also propel people-related risks as it creates an enabling environment for moral hazards to thrive which ultimately drive the occurrence of operational risk events (Knežević, 2013). For example, banks staff are usually very aggressive to onboard customers when there is a bonus incentive for performance. They sign off on risky transactions and circumvent higher level approvals (Xu, Tan & Netessine, 2017). For these risks to be managed however, there is need to have skilled and experienced risk officers who will continually identify emerging risks and put appropriate mitigants in place to reduce occurrence of operational risk events (Accenture, 2015). There is also a need to ensure that skills of risk officers are up scaled to be able to identify and detect likely frauds. The necessary tools that can assist in early detection of operational risk events should also be made available to the staff (BCBS, 2011).

IT system is another main driver of operational risk in banks which may crystallize in form of IT system hacks, system breaches/compromise, system downtime/system crash and over reliance on third party IT providers. Unlike the other drivers, the risk events caused by IT systems are comparatively easy to spot though they may vary from hardware to software IT issues (Knezevic, 2013). Though technological advancement and the need to ensure data security in banks have increased reliance on third parties service providers; especially in the area of cloud computing, however, these IT services exposes banks to risk of outages and its consequential effect on financial losses and customer service relationships. For example, in 2016, HSBC bank had a 2-days service outage where millions of its retail customers could not access their accounts. Also, in 2015, service downtime on the bank's electronic payment platform affected thousands of its customers (Risk Net, 2019). Another example is the 2010 prolonged disruption on the Swedbank's system which affected its online services (including ATM, card systems and internet banking system). After the event, the bank had to indemnify affected customers in form of restitution and eventually implemented some improvements (Jongh, Jongh, Jongh & Vuuren, 2013). Another is the Bangladesh Bank heist where some hackers exploited vulnerabilities in the bank's Swift financial communications network (IT systems) to steal \$81mn from the central bank account maintained by the bank and \$3.1mn theft from Tesco Bank customers' accounts (9,000 customers) after a data breach (Risk Net, 2019).

Internal process and procedure is the most challenging driver of risk in banks mainly because process risk is intricately linked to people risks and often difficult to distinctively separate (Abdullah, Farouk & Bassam, 2018; Knezevic, 2013). It is usually very difficult to separate the risk caused by failed internal processes from those caused by people. The potential factors of operational risks arising from failed internal process usually stems from inadequate or lack of clarity to staff on their responsibilities or duties, process gaps (i.e. absence of defined process for some activities) and overlapping duties (Knezevic, 2013). These failures will often manifest in form of omissions and work inefficiencies. Also, the design of some processes adopted by banks may have some loopholes which may expose the bank to risk of process manipulation by unscrupulous staff (Abdullah, Farouk & Bassam, 2018). Unlike other drivers of operational risks, loopholes in internal processes are often difficult to detect and usually require a strong commitment and right disposition of management to identify them and eventually resolve them (Knezevic, 2013).

### **Empirical Review and Hypothesis Development**

Operational risk in Nigerian banking industry gained more attention after the banking consolidation era mainly because of the enormous and increasing amount of operational losses recorded by banks (Owojori, Akintoye & Adidu, 2011). In Nigerian Banks, several studies have affirmed that majorly, operational losses are caused by management failure (people) and non-adherence to stipulated processes & policies. For example, Abdullahi's 2013 study (as cited in Zidafamor, 2016) highlighted that operational risk in Nigerian Banks is largely aggravated by ignorance and flagrant violation of relevant policies by Bank's management. Some of the bank's management are either not well-informed of the risks inherent in banking activities or have refused to comply with applicable policies that protect the bank's operations from possible operational losses. Ayodele and Alabi (2014) also asserted that Nigerian banks are riddled with high operational risk culminating from fraud and forgery incidences which they adduced to poor risk identification in the banking operations or non-adherence to regulatory directives by the management teams. Owojori, Akintoye and Adidu (2011) study also corroborated the fact that operational losses in Nigerian banking industry mainly stem from weak internal processes and retention of staff with high inclination for fraudulent activities. These factors are common for most banks in Nigeria with high operational losses. The weaknesses in internal process often manifest in form of control lapses like high level of sticky unreconciled items, inadequate dormant account management, non-compliance with dual controls around cash/high valuable assets and inadequate audit of bank's online presence. Bank staff also drive operational risk and contribute to operational loss through frauds and forgeries. Analysis of the frauds committed by staff revealed the commonest frauds as forged cheques, unauthorized credits, fraudulent transfers/withdrawals, cash suppression and cash theft. Surprisingly also, the employees that are involved in these frauds are the higher-level management staff. In fact, the trend of managers involved in this crime is on the increase. Ayodele and Alabi (2014) also insinuated that the high operational risk events recorded by Nigerian banks were mainly due to breach of defined process and ignorance or flagrant neglect of regulatory directives issued to mitigate these risks by management staff. These lapses often create an enabling environment for fraud and forgeries. CBN (2014) however asserted that, aside poor governance, operational risk in Nigerian deposit money banks are caused by poor IT infrastructure. To manage internal fraud risk however, banks take fidelity insurance policies to reduce the effect of insider frauds. To manage the process driven risks, there is need to enhance operational risk management practices and improve control processes. Regulators also need to ensure regular audit of involvement of board and top management staff of banks in operational risk management as they constitute the most important mitigating factor for operational risks. The effective involvement of the management teams would ensure establishment of appropriate and effective internal process and controls in the bank (Owojori, Akintoye & Adidu, 2011).

The research hypothesis is formulated in this section. From the review of the literatures, we identified three (3) dominant drivers revolving around people (staff), internal processes/policies and IT systems. This is summarized in Table 1.

**Table 1:** Drivers of Operational Risks

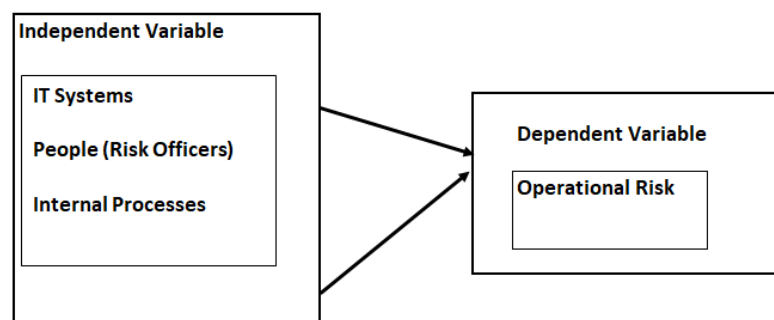
S/N	Authors and Year	Drivers Identified	Summary of Key Drivers by Basel Categorization
1	Kamau (2010) as cited in Siminyu, Clive & Musiega, 2017	- Automated technology - Quality of staff and management support	- IT Systems - People
2	Owojori, Akintoye and Adidu (2011)	- Weak internal processes - Retention of staff with high inclination for fraudulent activities	- Internal Processes - People
3	Abdullahi (2013)	- Ignorance and flagrant violation of relevant policies by Bank's management - Inadequate knowledge of risks inherent in banking activities by Bank's Management or blatant refusal to comply with applicable policies.	- Internal Processes - People
4	Hemrit and Arab (2013)	- Shortages of skilled staff - Inadequate process and documentation and implementation	- Internal Processes - People
5	Ayodele and Alabi (2014)	- Breach of defined process - Ignorance or flagrant neglect of applicable regulatory directives management staff	- Internal Processes - People
6	CBN (2014)	- Poor governance - IT infrastructure	- People - Internal Processes - IT Systems
7	Abdullah, Farouk and Bassam (2018)	- People's risk	- People
8	Sultania (2018)	- Human error - IT failures - Failures of internal processes	- People - Internal Processes - IT Systems

Source: Compiled by Researchers

Based on the results as shown in Table 1 and the objective of this study, the understated hypothesis was formulated:

Ho: Quality of risk personnel, IT system and internal processes are not main drivers of operational risks in banks.

Hi: Quality of risk personnel, IT system and internal processes are main drivers of operational risks in banks.



**Figure 1:** Research Framework

## Research and Methodology

A cross-sectional survey design was used to investigate the extent to which each operational risk driver contributes to operational risk in Nigerian commercial banks. The population of the study consisted of the 20 licensed commercial banks in Nigeria; as at the time of the study, however, at the initial stage, quota sampling technique was used to stratify the population along their years of operations into ‘old’, ‘not so old’ and ‘relatively new’ categories and two banks were thereafter selected from each category. The banks selected for the study include: First Bank Nig. Ltd (Founded in 1894), Union Bank Plc (Founded in 1917), Access Bank Plc (Founded in 1989), Fidelity Bank (Founded in 1988), Zenith Bank (Founded in 1990) and Stanbic IBTC (Founded in 1991). Thereafter, the purposive and convenient sampling techniques were used to select the operational risk officers that responded to the

survey. According to Bryman (2012), the purposive sampling allows the researcher to select relevant samples with reference to the research objectives. This is very relevant for the study as it ensures selection of respondents with specialized/in-depth knowledge of the operational risk management practices of their respective banks. The convenience sampling technique based on availability, cost and proximity was used in selecting respondents that were interviewed. To ensure fair and credible representation however, only interviewees who have spent a minimum of seven (7) years on the operational risk management role and are of the Assistant Manager Grades and above were selected.

### **Data Collection Instrument**

The study used questionnaire as the research collection instrument. The statements on the questionnaires were developed from the review of relevant literatures, research questions, aim of study and the hypothesis. The questionnaires were administered by hand and by email to the respondents. Some of the respondents who responded via email were also selected and interviewed physically to validate their responses.

The questionnaire was in four (4) sections. The first section contained general introduction of the research objectives to the respondents. The second was designed to gather relevant information on how internal process influences operational risk management in banks. The third sections collected useful information about how IT systems drive operational risk in banks and the last section was developed to collect information on how people (operational risk officers) contribute to operational risk in banks. Apart from the first section of the questionnaire, the questions were based on five-point Likert scale ratings of individual factors where the respondents were asked to rank on a scale of 1-5 (where 1 indicates “Strongly Disagree” and 5 indicates “Strongly Agree”) on the extent to which they agreed with the statements made.

Li (2016) asserted that the most important factors to consider when developing and testing a questionnaire to be used for a study is validity and reliability; as these factors have significantly influence on the quality of measurement and data collection. He defined validity as the extent to which an instrument accurately measures what it is intended to measure, and reliability was defined as the extent to which an instrument produces consistent results. To affirm reliability of the questionnaire administered, the test re-test reliability pilot test was conducted on selected respondent twice (within an interval of two-weeks) before adoption and administration of the questionnaires. The questions were also developed to cover the main construct of interest via face and content validity method. To achieve this, sample questions were developed from relevant literature reviews and the hypotheses indicated for test. These questions were then assessed meticulously by checking the questions developed against the conceptual definition constructs under investigation.

For this study, five (5) questionnaires were administered each to the Operational Risk Management Department of the six (6) selected banks totaling 30 respondents. Responses received from the selected banks are as follows: Union Bank (4 respondents), First Bank Plc. (5 respondents), Access Bank Plc. (3 respondents), Stanbic IBTC (3 respondents), Fidelity Bank (3 respondents) and Zenith Bank (3 respondent) totaling 21 retrieved questionnaires. To further investigate and validate the responses provided on the questionnaires which were administered via emails, follow up interview sessions were held with four (4) of such respondents. The respondents were selected based on convenience (i.e. availability, cost and proximity of the respondents) and their years of experience on the operational risk management desk. To ensure fair representation however, selection was done from four (4) of the sampled banks. The respondents interviewed have spent a minimum of seven (7) years on the operational risk management role and are of the Assistant Manager Grades and above. During the interview, a set of open-ended questions (coined from major themes of the questionnaire) were administered to the respondents and their responses were noted. The researchers compared the output of the interview with the initial responses of the respective respondents and concluded that the responses were consistent with the information provided on the questionnaires initially administered. Based on this, the postal responses were upheld as reliable and included in the analysis.

### **Ethical issues**

The respondents were assured of their anonymity and the confidentiality of information provided. They were duly informed about the objectives of this study and assured that there will be no risks involved if they participate. They were also informed of their rights to consent voluntarily, decline or withdraw from participating whenever they want to without any consequence. The wordings on the survey form were free of bias towards any group (e.g., age, ethnicity, race, sexual orientation, gender, etc.). Measures were also put in place to protect respondents’ anonymity by ensuring the non-disclosure of the respondents’ names on the questionnaires. The objectives and benefits of the study were also highlighted and attached to the survey form and consent of participants were duly obtained.

### **Findings**

The data analysis was based on the 21 questionnaire responses received which represents a 70% response rate. This is above the 60% acceptable response rate as per Mangione’s 1995 study (as cited in Bryman, 2012). The researcher therefore considers the 70% response rate acceptable and generalised the outcome of the study based on the returned questionnaires.

The data gathered was summarized, coded and tabulated. Data presentation was done using combination of descriptive statistics, graphs and some nonparametric inferential statistics to identify trends and draw conclusions. This was then analysed with the aid of

MS Excel and Statistical Packages for the Social Sciences (SPSS) Version 21.0. The results of data analysed are presented in the tables and charts below. The respondents' demographic is presented in Table 2.

**Table 2:** Respondents Demographic Characteristics and Classification

Variable	Frequency		(%)
How long have you been in the risk management function?	1-5 years	7	33
	6 to 10 years	10	48
	11years & above	4	19
	Total	21	100
Which management level best describes your role?	Middle level	13	62
	Low level	8	38
	Total	21	100
Level of education (Multiple response allowed)	Bachelor's degree only	7	33
	Bachelor's degree & Masters' degree	6	29
	Bachelor's degree & Professional Certificate	3	14
	Bachelor's degree, Masters' degree & Professional Certificate	5	24
	Total	21	100

**Source:** Field Survey, 2019.

The Table 2 above shows how long respondents have been in the operational risk management function. 33%, 48% and 19% of the respondents have spent between 1 to 5 years, 6 to 10 years and 11 years and above respectively in the operational risk management function. This response suggests that on the average, respondents have spent up to 7 years in the operational risk management function which implies that the respondents are relatively experienced in the risk management field.

Table 2 also indicated that 62% of the respondents are middle level staff while 38% are low level staff. This implies that majority of the respondents belong to middle level management.

Furthermore, it (Table 2) also highlights the educational level of the respondents. 33% of the respondents have only bachelors' degree or its equivalent, 29% have both bachelor's degree and masters' degree, 14% have both bachelor's degree and at least one professional qualification while 24% have Bachelor's degree, Master degree and relevant professional qualifications. This also suggests that 43% (29% plus 14%) of the respondents have at least two (2) degrees. This implies that majority of the respondents possess requisite qualification and exposure and can therefore be considered to be experts in operational risk management field.

Table 3 shows that 19% of the respondents agreed that the bank has clearly-stated risk management framework, processes and policies in place while 81% respondents strongly agreed. The analysis revealed that 28% of the respondents agreed that processes/policies/procedures are clearly documented and made available to all staff, 62% respondents strongly agreed while 10% respondents were neutral. 19% strongly agreed, 47% respondents agreed, 24% respondents were neutral, while 10% disagreed that all processes/policies/procedures/controls are regularly reviewed (at least once in a year) to reflect changes in the business environment. The analysis also shows that 34% of the respondents strongly agreed, 28% respondents agreed, 10% were neutral while 28% respondents disagreed that risk information are promptly and always communicated throughout the bank.

Table 3 also revealed that 90% of the respondents strongly agreed while 10% of the respondents agreed that there is a risk management committee saddled with the task of discussing and resolving risk issues in the bank. 95% of the respondents strongly agreed while 5% of the respondents agreed that the risk management committees meet at least once every month. The analysis also indicates that 52% strongly agreed, 14% of the respondents agreed, 10% were neutral and 24% disagreed that there are cases of ambiguity in the documented process.

In addition, the results (Table 3) revealed that 76% of the respondents strongly agreed while 24% respondents agreed that there is an effective sanction grid for ethical & professional breaches. The analysis also indicates that 57% of the respondents strongly agreed, 33% agreed while 10% were neutral that the bank has clearly defined delegated roles and responsibilities for all business processes and that all processes have clear owners. The result also revealed that 19% of the respondents strongly agreed, 24% agreed, 28% were neutral, 19% disagreed while 10% of the respondents strongly disagreed that management sometimes override approved processes and controls.

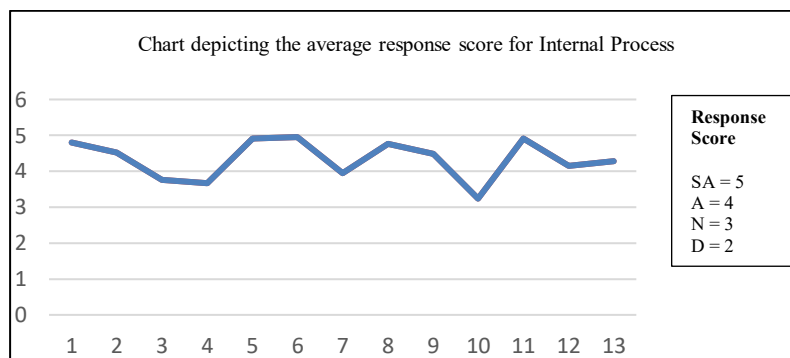
**Table 3:** Analysis of Internal Process

Statements	Frequency & Percentage (%)						Descriptive Statistics	
	SD %	D %	N %	A %	SA %	Total %	Mean	Standard Deviation
1. The bank has clearly-stated risk management framework, processes and policies in place	0% (0)	0% (0)	0% (0)	19% (4)	81% (17)	100%	4.8	0.4
2. Processes/policies/procedures are clearly documented and made available to all staff	0% (0)	0% (0)	10% (2)	28% (6)	62% (13)	100%	4.5	0.7
3. All Processes, policies, procedures, controls are regularly reviewed (at least once in a year) to reflect changes in the business environment	0% (0)	10% (2)	24% (5)	47% (10)	19% (4)	100%	3.8	0.9
4. Risk information are promptly and always communicated throughout the bank	0% (0)	28% (6)	10% (2)	28% (6)	34% (7)	100%	3.7	1.2
5. There is a Risk Management Committee saddled with the task of discussing and resolving risk issues in the bank	0% (0)	0% (0)	0% (0)	10% (2)	90% (19)	100%	4.9	0.3
6. The Risk Management Committees meet at least every month	0% (0)	0% (0)	0% (0)	5% (1)	95% (20)	100%	5.0	0.2
7. There are cases of ambiguity (i.e. not clearly defined) in the documented process	0% (0)	24% (5)	10% (2)	14% (3)	52% (11)	100%	3.9	1.3
8. There is an effective sanction grid for ethical & professional breaches	0% (0)	0% (0)	0% (0)	24% (5)	76% (16)	100%	4.8	0.4
9. The bank has clearly defined delegated roles and responsibilities for all business processes and all processes have clear owners	0% (0)	0% (0)	10% (2)	33% (7)	57% (12)	100%	4.5	0.7
10. Management sometimes override approved process/controls	10% (2)	19% (4)	28% (6)	24% (5)	19% (4)	100%	3.2	1.3
11. There are approved guidelines for the development and management of all products of the bank	0% (0)	0% (0)	0% (0)	10% (2)	90% (19)	100%	4.9	0.3
12. All exceptions (from audit, regulators, control functions) are centrally tracked till resolution	0% (0)	5% (1)	14% (3)	43% (9)	38% (8)	100%	4.1	0.9
13. All key processes are audited on a regular basis	0% (0)	10% (2)	10% (2)	24% (5)	56% (12)	100%	4.3	1.0

\*\*\*Strongly Disagree (SD), Neutral (N), Disagree (D), Agree (A), Strongly agree (SA). SA was ranked as 5 and SD as 1.

**Source:** Field Survey, 2019.

It was discovered that 90% of the respondents strongly agreed while 10% of the respondents agreed that there are approved guidelines for the development and management of all products of the bank. It was also discovered that 38% of the respondents strongly agreed, 43% of the respondents agreed, 14% were neutral while 5% disagreed that all exceptions (from audit, regulators, control functions) are centrally tracked till they are resolved. The analysis also indicates that 56% of the respondents strongly agreed, 24% agreed, 10% were neutral and 10% disagreed that all key processes are audited on a regular basis. Average response score for internal process risk officers is presented in Figure 1.



**Figure 1:** Average Response Score for Internal Process Risk Officers

Apart from statement 10, all the statements have mean scores above 3.6 which indicate that, majority of the respondents agreed with the statements made. The associated standard deviations are also relatively low indicating low variability in their responses. For statement 10 which inquired if management sometimes overrides approved process/controls however, the mean score was 3.2, this indicates that majority of the respondents were indifferent. This also implies that bank management sometimes overrides approved processes/controls. The standard deviation of 1.3 was also recorded for this statement which suggests relatively low variability in the responses of the respondents.

**Table 4:** Analysis of IT System

Statements	Frequency & Percentage (%)					Descriptive Statistics		
	SD	D	N	A	SA	Total	Mean	Standard Deviation
1. Banks record some form of operational losses when there is a downtime	10% (2)	24% (5)	24% (5)	14% (3)	28% (6)	100%	3.3	1.4
2. Unplanned outages contribute greatly to operational losses in banks	10% (2)	4% (1)	38% (8)	38% (8)	10% (2)	100%	3.3	1.1
3. Failure of critical applications can lead to operational loss	0% (0)	0% (0)	0% (0)	33% (7)	67% (14)	100%	4.7	0.5
4. Loss of data arising from system glitches can have significant legal and financial impacts	0% (0)	0% (0)	0% (0)	43% (9)	57% (12)	100%	4.6	0.5
5. Inadequate data backup exposes the bank to huge potential operational losses	0% (0)	0% (0)	0% (0)	29% (6)	71% (15)	100%	4.7	0.5
6. Banks with effective data center/disaster recovery centers can effectively manage operational losses	0% (0)	0% (0)	10% (2)	10% (2)	80% (17)	100%	4.7	0.6
7. Basic services can be provided to Customers when there is a prolonged system downtime	10% (2)	14% (3)	5% (1)	24% (5)	47% (10)	100%	3.9	1.4
8. Inadequate data security exposes the bank to operational losses	0% (0)	0% (0)	0% (0)	33% (7)	67% (14)	100%	4.7	0.5
9. Bank has reasonable measures in place to prevent data loss or data interruption or unauthorized access to its network	0% (0)	0% (0)	0% (0)	43% (9)	57% (12)	100%	4.6	0.5
10. The response time for systems (i.e., time it takes system to process an input and produce an outcome) can lead to some form of operational losses	0% (0)	14% (3)	0% (0)	43% (9)	43% (9)	100%	4.1	1.0
11. Most bank activities are supported by IT system (Higher percentage of automation)	0% (0)	0% (0)	5% (1)	38% (8)	57% (12)	100%	4.5	0.6
12. Backups exist for existing critical IT System	0% (0)	0% (0)	0% (0)	38% (8)	62% (13)	100%	4.6	0.5
13. There are contingency sites available from which back-up systems can be employed if the location of the main site is impaired	0% (0)	0% (0)	0% (0)	29% (6)	71% (15)	100%	4.7	0.5
14. All new systems are thoroughly tested and run on a parallel basis with existing systems during their launch period	0% (0)	0% (0)	10% (2)	33% (7)	57% (12)	100%	4.5	0.7
15. IT staff are trained on operational risks	0% (0)	10% (2)	24% (5)	33% (7)	33% (7)	100%	3.9	1.0
16. There is a direct relationship between system downtime and operational loss	0% (0)	14% (3)	29% (6)	47% (10)	10% (2)	100%	3.5	0.9
17. Internal Audit Department regularly conducts system audit.	0% (0)	0% (0)	0% (0)	43% (9)	57% (12)	100%	4.6	0.5

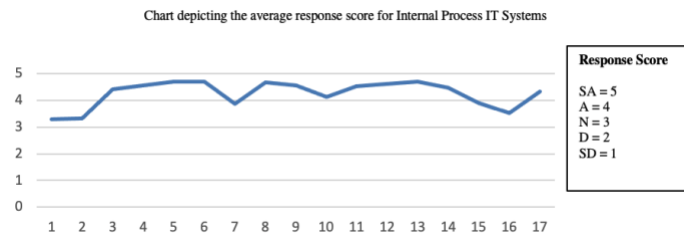
\*\*\*Strongly Disagree (SD), Neutral (N), Disagree (D), Agree (A), Strongly agree (SA). SA was ranked as 5 and SD as 1.

**Source:** Field Survey, 2019.

Table 4 shows that 28% of the respondents strongly agreed that banks record some form of operational losses when there is a downtime, 14% respondents agreed, 24% respondents were neutral, 24% respondents disagreed while 10% respondents strongly disagreed. The analysis revealed that 10% of the respondents strongly agreed that unplanned outages contribute greatly to operational losses in banks, 38% agreed, 38% were neutral, 4% disagreed while 10% strongly disagreed. It was also discovered that 67% of the respondents strongly agreed, 33% agreed that failure of critical applications can lead to operational loss. The analysis above shows that 57% of the respondents strongly agreed, while 43% agreed that loss of data arising from system glitches can have significant legal and financial impacts. The results (Table 4) also indicated that 71% of the respondents strongly agreed while 29% of the respondents agreed that inadequate data backup exposes the bank to huge potential operational losses.



It was also discovered that 80% of the respondents strongly agreed, 10% of the respondents agreed while 10% respondents were neutral that banks with effective data center/disaster recovery centers can effectively manage operational losses. The results also revealed that 47% of the respondents strongly agreed, 24% agreed, 5% were neutral, 14% disagreed while 10% strongly disagreed that basic services can be provided to customers when there is a prolonged system downtime. 67% of the respondents strongly agreed while 33% of the respondents agreed that inadequate data security exposes the bank to operational losses; 57% of the respondents strongly agreed, while 43% of the respondents agreed that bank has reasonable measures in place to prevent data loss or data interruption or unauthorized access to its network. The analysis also shows 43% of the respondents strongly agreed, 43% agreed, while 14% of the respondents disagreed that the response time for systems (i.e., time it takes system to process an input and produce an outcome) can lead to some form of operational losses. It was discovered that 57% of the respondents strongly agreed, 38% agreed while 5% of the respondents were neutral that most bank activities are supported by IT system (Higher percentage of automation). Furthermore, 62% of the respondents strongly agreed, while 38% of the respondents agreed, that backups exist for existing critical IT System. The result also shows that 71% of the respondents strongly agreed that there are contingency sites available from which back-up systems can be employed if the location of the main site is impaired, while 29% respondents agreed. The analysis revealed that 57% of the respondents strongly agreed that all new systems are thoroughly tested and run on a parallel basis with existing systems during their launch period, 33% agreed, 10% were neutral. It was also discovered that 33% of the respondents strongly agreed, 33% agreed, 24% were neutral while 10% respondents disagreed that IT staff are trained on operational risks; 10% of the respondents strongly agreed, while 47% agreed, 29% were neutral, while 14% disagreed that there is a direct relationship between system downtime and operational loss; and 57% of the respondents strongly agreed, 43% agreed that Internal Audit Department regularly conducts system audit. The average response score for internal process IT system is present in Figure 2.



**Figure 2:** Average response score for Internal Process IT Systems

Apart from statements 1 and 2, all the statements have mean scores above 3.5 which indicates that, majority of the respondents agreed with the statements made with minimal variability in their responses. However, statements 1 and 2 have mean scores of 3.3; this indicates that majority of the respondents are indifferent to the statements which implies that both system downtime and unplanned outages do not necessarily contribute greatly to operational losses in banks.

**Table 5:** Results of Risk Officers Data

Risk Officers	Frequency & Percentage (%)						Descriptive Statistics	
	SD (%)	D (%)	N (%)	A (%)	SA (%)	Total (%)	Mean	Standard Deviation
1. The bank has adequate manning level for risk management functions	0	43%	24%	28%	5%	100	4.0	1.0
2. The Risk Officers have necessary knowledge and skills to identify relevant risks associated with banking activities	0	0	14%	71%	15%	100	4.0	0.5
3. Risk Officers are specifically trained on complex products to be able to identify related risks	0	10%	19%	47%	24%	100	3.9	0.9
4. There is appropriate tone from the Board and top Management that engenders a positive risk behaviour & culture in the bank	0	0	10%	52%	38%	100	4.3	0.6
5. Operational Risk Staff are regularly trained on emerging operational risk issue and how to identify them	5%	28%	24%	19%	24%	100	3.3	1.3
6. Operational Risk Staff have in-depth understanding of internal policies, external regulations and bank's products/processes	0	0	14%	57%	29%	100	4.1	0.7
7. Operational Risk Staff are skilled in identifying risks and effectively work with Business Owners to develop appropriate mitigants	0	19%	0	57%	24%	100	3.9	1.0
8. Board & Management Team have the right skills and exposure needed to effectively manage the risks of the bank	0	0	5%	62%	33%	100	4.3	0.6

\*\*\*Strongly Disagree (SD), Neutral (N), Disagree (D), Agree (A), Strongly agree(SA). SA was ranked as 5 and SD as 1.

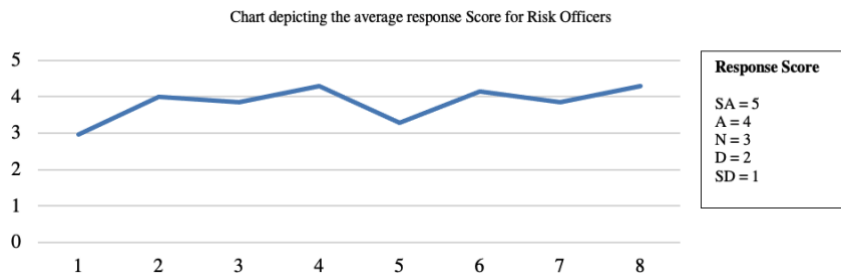
**Source:** Field Survey, 2019.

Table 5 above revealed that 5% of the respondents strongly agreed, 28% agreed, 24% were neutral while 43% of the respondents disagreed that the bank has adequate manning level for risk management functions. It was also discovered that 14% of the respondents strongly agreed, 71% agreed, while 15% were neutral that Risk Officers have necessary knowledge and skills to identify relevant risks associated with banking activities.

The table shows that 24% of the respondents strongly agreed, 47% agreed, 19% were neutral, while 10% disagreed that Risk Officers are specifically trained on complex products to be able to identify related risks. The table revealed that 38% of the respondents strongly agreed, 52% agreed, while 10% were neutral that there is appropriate tone from the Board and top Management that engenders a positive risk behaviour & culture in the bank.

The analysis in table above revealed that 24% of the respondents strongly agreed, 19% agreed, 24% were neutral, 28% disagreed while 5% of the respondents strongly disagreed that Operational Risk Staff are regularly trained on emerging operational risk issue and how to identify them. It was discovered that 29% of the respondents strongly agreed, 57% agreed while 14% of the respondents were neutral that Operational Risk Staff have in-depth understanding of internal policies, external regulations and bank's products/processes. It was also discovered that 24% of the respondents strongly agreed, 57% of the respondents agreed, while 19% disagreed that Operational Risk Staff are skilled in identifying risks and effectively work with Business Owners to develop appropriate mitigants.

The table above also shows that 33% of the respondents strongly agreed, 62% agreed, while 5% were neutral that Board & Management Team have the right skills and exposure needed to effectively manage the risks of the bank. The summary of average response score for risk officers is presented in Figure 3.



**Figure 3:** Average response Score for Risk Officers

All the statements, except statement 1 and 5, have mean scores above 3.80 which indicates that, majority of the respondents agreed with the statements made with insignificant variability in their responses.

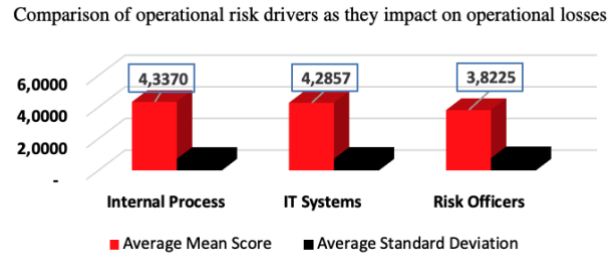
For statement 1 which inquired if the bank has adequate manning level for risk management functions, the mean score was 3.0 which suggests that many of the respondents believe that the banks' risk management functions are not adequately manned. Statement 5 inquired whether Operational Risk Management Staff are regularly trained on emerging operational risk issue and how to identify them, the average score was 3.3. This suggest that on the average, the respondents have indifferent opinions. This also implies that the Risk Officers are not adequately and regularly trained on emerging operational risk issues. There is need to ensure adequate manning level and trainings for risk management staff to enable them effectively cover all critical risk areas with minimal errors. According to Abdullah, Farouk & Bassam (2018) and Knežević (2013), high staff workload and inadequate trainings increases error rates and have grave impact on operational losses.

**Table 6:** Average mean score and standard deviation of drivers of operational risk

Risk drivers	Average mean score	Average standard deviation
Internal Process	4.3370	0.7347
IT Systems	4.2857	0.7406
Risk Officers	3.8225	0.7789

**Source:** Field Survey, 2019

Average response scores for the different drivers were computed with score of 5 representing strong agreement to the statements that the driver influences operational risk levels and score of 1 representing strong disagreement. From Table 6 above, the mean scores for the three drivers were above 3.80 which indicates that on the average, majority of the respondents believe that Internal Process, IT systems and Quality of Risk Officer impact on operational risk levels and by extension determines operational losses recorded by banks. The average standard deviation was also relatively low and revolves around same level which indicates consistency in the opinions of the respondents. The comparison of drivers of operational risk as they impact on operational losses is presented in Figure 4.



**Figure 4:** Comparison of operational risk drivers as they impact on operational losses

Chart 4 above shows the comparison of operational risk drivers as they impact on operational losses. From the chart, Internal processes was shown as the driver that impacts on operational losses the most. This is consistent with the findings in the study done by Owojori, Akintoye and Adidu (2011) and Ayodele and Alabi (2014).

**Hypothesis Testing**

In line with the objective of this study, the following hypothesis was made:

Ho: Quality of risk personnel, IT system and internal processes are not main drivers of operational losses of banks.

To test this hypothesis, the mean values and confidence intervals were computed for each statement made to test whether Quality of risk personnel, IT system and internal processes are not main drivers of operational losses of banks. The computation was based on the 21 responses received from the Operational Risk management desks of the six (6) selected banks.

**Table 7:** Means of Responses and Confidence Intervals at 95% Significance Level

Statement no.	Internal Process		IT Systems		Risk Officers	
	Confidence Interval (C.I)	95% Lower and Higher C.I	Confidence Interval (C.I)	95% Lower and Higher C.I	Confidence Interval (C.I)	95% Lower and Higher C.I
1	0.1721	(5.3731, 5.7175)	0.5918	(2.6940, 3.8775)	0.3109	(3.5462, 4.1681)
2	0.2907	(4.2331, 4.8145)	0.4553	(2.8780, 3.7887)	0.2128	(3.4062, 3.8319)
3	0.3803	(3.3816, 4.1422)	0.2066	(4.4601, 4.8733)	0.3287	(3.5761, 4.2334)
4	0.5296	(3.1371, 4.1963)	0.2169	(4.3545, 4.7883)	0.4163	(2.5360, 3.3687)
5	0.1286	(4.7761, 5.0334)	0.1980	(4.5163, 4.9123)	0.2343	(4.5384, 5.0070)
6	0.0933	(4.8590, 5.0457)	0.2753	(4.4390, 4.9896)	0.3893	(3.4678, 4.2465)
7	0.5490	(1.4986, 2.5966)	0.6092	(3.2480, 4.4663)	0.2753	(4.0104, 4.5610)
8	0.1867	(4.5752, 4.9486)	0.2066	(4.4601, 4.8733)	0.5434	(2.7423, 3.8291)
9	0.2907	(4.1855, 4.7669)	0.2169	(4.3545, 4.7883)	0.2800	(3.8629, 4.4229)
10	0.5394	(2.2225, 3.3013)	0.4338	(3.7091, 4.5766)	0.4338	(3.4234, 4.2909)
11	0.1286	(4.7761, 5.0334)	0.2573	(4.2665, 4.7811)	0.2398	(4.0459, 4.5255)
12	0.3651	(3.7778, 4.5079)	0.2128	(4.4062, 4.8319)	N/A	N/A
13	0.4307	(3.8550, 4.7165)	0.1980	(4.5163, 4.9123)	N/A	N/A
14	N/A	N/A	0.2907	(4.1855, 4.7669)	N/A	N/A
15	N/A	N/A	0.4257	(3.4791, 4.3304)	N/A	N/A
16	N/A	N/A	0.3733	(3.1505, 3.8971)	N/A	N/A
17	N/A	N/A	0.2169	(4.3545, 4.7883)	N/A	N/A

**Source:** Field Survey, 2019 \* Response Score SA = 5, A = 4, N = 3, D = 2, SD = 1\*

From Table 7, the mean scores were compared with the confidence interval limits at 95% level of significance. It was noted that all the means fell within the computed lower and higher C.Is. This implies that majority of the respondents believed that Internal Processes, IT systems and Quality of Risk Officers are main drivers of Operational loss. Based on this, the null hypothesis was

rejected and the alternate hypothesis that Quality of risk personnel, IT system and Internal Processes are main drivers of operational losses of banks was accepted.

## **Discussion**

Analysis of the responses showed that most of the respondents have spent a minimum of 6 years on the operational risk management desk. Majority of the respondents were also discovered to be in the middle management cadre. Also, all the respondents have relevant first degrees and majority have relevant second degrees.

Analysis of the process related statements indicated that majority of the banks have clearly defined and approved risk management frameworks, policies, procedures, guidelines as well as defined roles and responsibilities. All respondents also agreed that there are risk management committees that sit at least once every month to discuss and resolve risks in the banks. All respondents also agreed that there is an effective sanction grid for ethical and professional breaches. However, responses received indicated that management sometimes override set controls. Analysis of the responses collected on the IT System related questions suggests that system outages and unplanned outages do not necessarily drive operational risks. All respondents however agreed that the failure of critical applications, loss of data arising from system glitches and inadequate data backup/security contribute greatly to the volume of operational losses recorded by banks. All respondents also agreed that their banks have reasonable measures in place to prevent data loss/interruption or unauthorized access to their IT networks as well as backups for critical IT System. Responses received also suggests that the banks have contingency sites available from which back-up systems can be employed if the location of the main site is impaired. They all stated that Internal Audit Department regularly conducts system audit.

Analysis of the responses collected on the Risk Officer category suggests that banks do not have adequate manning levels for their risk management functions. Also, majority of the respondents agreed that operational risk managers are not adequately and regularly trained on emerging operational risk issues and how to identify them. Majority of the respondents however agreed that there is an appropriate tone from the Board and top Management that engenders a positive risk behaviour and culture in the bank. Majority also agreed that the Board and Management Teams have the right skills and exposure needed to effectively manage the risks of the banks.

Most of the respondents agreed that Operational Risk Staff have in-depth understanding of internal policies, external regulations and bank's products/processes and are skilled in identifying related risks and effectively work with Business Owners to develop appropriate mitigants.

Further analysis of responses received on the three operational risk drivers indicated that internal process has the greatest impact on operational loss, followed by IT systems and then quality of risk officers.

The findings of the study support that of Abdullah et al, (2018) which asserted that inadequately trained staff and low manning levels can lead to errors and inability of the staff to carry out planned activities at an acceptable level. To mitigate these risks, Operational Risk Officers needs to be regularly trained; especially on emerging risk issues to arm them with the required skills that will enhance their effectiveness in managing the risks of the bank. Manning gaps should also be filled with officers that have relevant experiences and skill-sets required to proactively identify potential risk events and suggest possible remediation plans.

As evidenced by the findings of this study, lapses in bank's internal process constitute the main source of its operational risks and losses. It is recommended therefore that banks should develop and implement standard internal operating procedures for all its key activities and this should be reviewed at least on an annual basis to reflect possible changes. In alignment with the suggestion of Bain & Company, (2018), Banks should also ensure automation of these processes as much as possible to reduce manual intervention which will reduce errors and opportunities for fraud.

## **Conclusion**

Based on the findings of the research, the researchers concluded that quality of risk officers, IT systems and internal processes are main drivers of operational losses in banks, howbeit; internal process is the topmost driver of operational losses to banks followed by IT systems and then risk officers (staff). This study has two sets of implications for management practice. The first borders on the need for Bank Management to ensure regular review of critical processes in the bank and enhance controls around processes that have been identified as being prone to fraud or errors. The second involves incorporating mandatory trainings on emerging risks in the schedules of risk officers to facilitate effective identification of risks and enable them proffer plausible mitigants to address identified gaps. To tighten process controls also, Management should invest in robust IT infrastructure that will help automate processes and reduce manual intervention. This will reduce the associated risk of errors and fraud.

**Author Contributions:** Conceptualization, O.S.F, D.O.; methodology, O.S.F, D.O.; Data Collection, O.S.F, D.O.; formal analysis O.S.F, D.O.; writing—original draft preparation, O.S.F, D.O.; writing—review and editing, O.S.F, D.O.; Author has read and agreed to the published the final version of the manuscript.

**Institutional Review Board Statement:** Ethical review and approval were waived for this study, due to that the research does not deal with vulnerable groups or sensitive issues.

**Data Availability Statement:** The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy.

**Conflicts of Interest:** The author declares no conflict of interest.

## **Appendix**

List of Licensed Commercial Banks in Nigeria at the time of Study.

1	Access Bank Plc
2	Citibank Nigeria Limited
3	Diamond Bank Plc ***
4	Ecobank Nigeria Plc
5	Fidelity Bank Plc
6	First Bank Nigeria, Limited
7	First City Monument Bank Plc
8	Guaranty Trust Bank Plc
9	Heritage Banking Company Ltd.
10	Key Stone Bank
11	Polaris Bank
12	Providus Bank
13	Stanbic IBTC Bank Ltd.
14	Standard Chartered Bank Nigeria Ltd.
15	Sterling Bank Plc
16	SunTrust Bank Nigeria Limited
17	Union Bank of Nigeria Plc
18	United Bank for Africa Plc
19	Unity Bank Plc
20	Wema Bank Plc
21	Zenith Bank Plc

Source: CBN. Available at: <https://www.cbn.gov.ng/Supervision/Inst-DM.asp> Accessed 8th January 2019.

\*\*\* Diamond Bank Plc had been acquired by Access Bank Plc as at the time of this research. Source: Punch news. Retrieved from: <https://punchng.com/diamond-bank-confirms-merger-with-access-bank/> Accessed 8th January 2019.

## References

- Abdullah, A., Farouk, A., & Bassam, R. (2018). Operational risk management in financial institutions: An overview. *Business and Economic Research*, 8(2), 11-32. <https://doi.org/10.5296/ber.v8i2.12681>
- Accenture. (2015). Reaping the benefits of operational risk management. 1-16. Retrieved from [https://www.accenture.com/t20150715t045908\\_w\\_/mu-en/\\_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/industries\\_6/accenture-reaping-the-benefits-of-operational-risk-management.pdf](https://www.accenture.com/t20150715t045908_w_/mu-en/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/industries_6/accenture-reaping-the-benefits-of-operational-risk-management.pdf) (Accessed 5 February 2020)
- Ayodele, T. D., & Alabi, R. O. (2014). Risk management in Nigeria banking industry. *Research Journal of Finance and Accounting*, 5(2), 131-136.
- Bain & Company. (2018). Preventing disaster: How banks can manage operational risk. 1-12. Retrieved from [https://www.bain.com/contentassets/f0199ad9887e402cb37cd1fd316f5ee3/bain\\_brief\\_how\\_banks\\_can\\_manage\\_operational\\_risk.pdf](https://www.bain.com/contentassets/f0199ad9887e402cb37cd1fd316f5ee3/bain_brief_how_banks_can_manage_operational_risk.pdf) (Accessed 5 February 2020).
- Basel Committee on Banking Supervision (BCBS). (2011). Principles for the sound management of operational risk. Retrieved from <https://www.bis.org/publ/bcbs195.pdf> (Accessed 5 February 2020).
- Basel Committee on Banking Supervision (BCBS). (2014). Operational risk – Revisions to the simpler approaches. Retrieved from <https://www.bis.org/publ/bcbs291.pdf> (Accessed 16 January 2019).
- Bekele, B. (2015). The nexus between bank specific risk management practice and financial performance: A study on selected commercial banks in Ethiopia. [Online] SSRN. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2841206](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2841206) (Accessed 5 February 2020).
- Bryman, A. (2012). Social research methods (4th edition). Retrieved from [https://www.researchgate.net/profile/Yousef\\_Shahwan4/post/What\\_is\\_the\\_best\\_and\\_the\\_most\\_recent\\_book\\_in\\_medical\\_research\\_methodology/attachment/59d6525179197b80779aa90f/AS:511717807321088@1499014441133/download/Social\\_Research\\_Methods.pdf](https://www.researchgate.net/profile/Yousef_Shahwan4/post/What_is_the_best_and_the_most_recent_book_in_medical_research_methodology/attachment/59d6525179197b80779aa90f/AS:511717807321088@1499014441133/download/Social_Research_Methods.pdf) (Accessed 3 January 2019).
- CBN. (2014). Risk management in financial services industry. Understanding monetary policy40. Retrieved from <https://www.cbn.gov.ng/out/2016/mpd/understanding%20monetary%20policy%20series%20no%2040.pdf> (Accessed 01 February 2019).
- CIMA. (2008). Operational risk, topic gateway series no. 51. Retrieved from [http://www.cimaglobal.com/documents/importedddocuments/51\\_operational\\_risk.pdf](http://www.cimaglobal.com/documents/importedddocuments/51_operational_risk.pdf) (Accesses 16 January 2019).

- Fadun, O.S. & Oye, D. (2020). Impacts of operational risk management on financial performance: a case of commercial banks in Nigeria. *International Journal of Finance & Banking Studies*, 9(1), 22-25. <https://doi.org/10.20525/ijfbs.v9i1.634>
- Hemrit, W. & Arab, M.B. (2012). The major sources of operational risk and the potential benefits of its management. *Journal of Operational Risk*, 7(4), 71-92. <https://doi.org/10.21314/JOP.2012.115>
- Jongh, E. D., Jongh, D. D., Jongh, R. D., & Vuuren, G. V. (2013). A review of operational risk in banks and its role in the financial crisis. *South African Journal of Economic and Management Sciences*, 16(4), 364-382. <https://doi.org/10.4102/sajems.v16i4.440>
- Knežević, M. (2013). Operational risk – challenges for banking industry. *Economic Analysis*, 46(1-2), 40-52. Retrieved from [http://ebooks.ien.bg.ac.rs/367/1/2013\\_1\\_2\\_4.pdf](http://ebooks.ien.bg.ac.rs/367/1/2013_1_2_4.pdf)
- Li, Y. (2016). How to determine the validity and reliability of an instrument. Retrieved from <https://blogs.miamioh.edu/discovery-center/2016/11/how-to-determine-the-validity-and-reliability-of-an-instrument/> (Accessed 3 April 2019).
- Muriithi, J. G. (2016). Effect of financial risk on financial performance of commercial banks in Kenya. Retrieved from <http://ir.jkuat.ac.ke/bitstream/handle/123456789/2376/Jane%20Gathiga%20Muriithi%20Phd%20Finanace%20Thesis%202016.pdf?sequence=3&isAllowed=y> (Accessed 15 February 2019).
- Ng'aari, E. W. (2016). Effect of risk management practices on profitability of listed commercial banks in Kenya. Retrieved from <http://41.89.49.13:8080/xmlui/bitstream/handle/123456789/1157/Ngaari-Effect%20Of%20Risk%20Management%20Practices%20On%20The%20Profitability%20Of%20Listed%20Commercial%20Banks%20In%20Kenya.pdf?sequence=1&isAllowed=y> (Accessed 14 March 2019).
- Owojori, A. A., Akintoye, I. R., & Adidu, F.A. (2011). The challenge of risk management in Nigerian banks in the post consolidation era. *Journal of Accounting and Taxation*, 3(2), 23-31.
- Pakhchanyan, S. (2016). Operational risk management in financial institutions: A literature review. *International Journal of Financial Studies*, 4(20), 1-21. <http://dx.doi.org/10.3390/ijfs4040020>
- Radu, A. N., & Olteanu, A.C. (2009). The operational risk management. Retrieved from <http://www.asecu.gr/files/RomaniaProceedings/54.pdf> (Accessed 17 January 2019)
- Risk Net (2018). Top 10 op risk losses of 2017: Crisis-era fines abate. Retrieved from <https://www.risk.net/comment/5384771/top-10-op-risk-losses-of-2017-crisis-era-fines-abate> (Accessed 12 February 2020).
- Risk Net (2019). Top 10 operational risks for 2019. Retrieved from <https://www.risk.net/risk-management/6470126/top-10-op-risks-2019> (Accessed 12 February 2020)
- Risk Net (2019). Top 10 operational risks for 2017. Retrieved from <https://www.risk.net/risk-management/operational-risk/2480528/top-10-operational-risks-for-2017> (Accessed 11 March 2019)
- Simamora, R. J., Oswari, T. (2019). The effects of credit risk, operational risk and liquidity risk on the financial performance of banks listed in Indonesian stock exchange. *International Journal of Economics, Commerce and Management*, 7(5), 182-193.
- Siminyu, M., Clive, M., & Musiega, M. (2017). Influence of operational risk on financial performance of deposit taking savings and credit co-operatives in Kakamega County. *International Journal of Management and Commerce Innovations*, 4(2), 509-518.
- Sultania, S. (2018). 11 major risks faced by banks in 2018 and beyond. Retrieved from <https://gomedici.com/risks-in-the-banking-industry-faced-by-every-bank/> (Accessed 12 March 2019)
- Tandon, D., & Mehra, Y. S. (2017). Impact of ownership and size on operational risk management practices: a study of banks in India. *Global Business Review*, 18(3), 795–810. <https://doi.org/10.1177/0972150917692207>
- Xu, Y., Tan, T. & Netessine, S. (2017). When is the root of all evil not money? the impact of load on operational risk at a commercial bank. *SMU Cox School of Business Research Paper No. 18-13*. <http://dx.doi.org/10.2139/ssrn.3075452>
- Zidafamor, E. (2016). Risk management in Nigerian financial institutions. Retrieved from <https://www.researchgate.net/publication/301891410> (Accessed 4th February 2019)

**Publisher's Note:** Bussecon International stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Bussecon Review of Social Sciences by [Bussecon International Academy](#) is licensed under a [Creative Commons Attribution 4.0 International License](#).