OPERATIONAL RISK MANAGEMENT PRACTICES AND FRAUD IN COMMERCIAL BANKS IN KENYA

BY:

MARTIN RUNO NGOTHO

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF AWARD OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION, FACULTY OF BUSINESS AND MANAGEMENT SCIENCES UNIVERSITYOF NAIROBI

2023

DECLARATION

The idea for the project was from my own creation. It has never been submitted for a degree.

Signature _____ Date: 30TH NOVEMBER 2023

Martin Runo Ngotho

D61/70713/2007

The idea has been sent in for review, and it has received my approval in my capacity as Supervisor.

Signature _____ Date: **30th November, 2023**

Angela Wairimu Kaguara

Lecturer

Department of Management Science and Project Planning

University of Nairobi

DEDICATION

I would want to thank my family for all of the love, support, patience, encouragement, and understanding they have shown me during this study effort.

ACKNOWLEDGMENT

My first expression of appreciation belongs to God. The second thing I'd want to do is thank my family, my parents, and my siblings for their unflinching encouragement and support during my whole schooling process. In the second place, I'd want to give thanks to my Supervisor, Ms. Angela Wairimu Kaguara who was a huge help in terms of the project's development and monitoring. I also would like to appreciate my Moderator, Dr. Thomas Ombati whose input and guidance was instrumental in final document. In conclusion, I would like to recognize and appreciate the faculty of business and management sciences, as well as the community of the University of Nairobi.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AVS	Address Verification Service
BCBS	Basel Committee on Banking Supervision
BCCI	Bank of credit and commerce international
BIS	Bank of International Settlement
CBs	Commercial Banks
CBK	Central Bank of Kenya
CVV	Card Verification Value
EFT	Electronic Funds Transfer
IT	Information Technology
IRM	Institute of Risk Management
KBA	Kenya Banker Association
ORM	Operational Risk Management
ORMP	Operational Risk Management Practices
PIN	Personal Identification Number
PWC	Price Water house cooper
ROA	Return on Assets
ROE	Return on Equity
RSA	Risk Self-Assessment
TDA	Theory of Differential Association
VIF	Variance Inflation Factor

ABSTRACT

Operational risk continuously evolves and occurs in different types. In recent years, the importance of operational risk for banks has been increasing due to the products and methods which are very complex. Therefore this study undertakes to investigate the effect of operational risk management practices on bank fraud among commercial banks in Kenya. The population that was accessed consisted of all commercial banks as of the 31st of December, 2022 which had operated for at least 5 years. The study was conducted via the use of a census survey and primary data was used to collect and review information in order to fulfill the requirements of this investigation. From the results there was an indication that the correlation between the bank fraud when compared operational risk management practices as measured by the five variables of operational risk was negative. The research results also indicated that there is a strong positive relationship, thus a very high degree of correlation. A high R value is an indication that the model fits the data very well; in this case R value is 0.593. This implied that 59.3% of the variation in bank fraud as measured by computer fraud, payment fraud and credit card fraud was due to operations risk assessment, operational risk identification, operational risk measurement, operational risk monitoring and operational risk mitigation. While, 40.7% was due to other factors not covered in the model. The research findings are important to all the financial institutions in terms understanding the impact of sound operational risk management practices on the fraud and performance of financial institutions. The financial institutions can use this study for training purposes and improving employee awareness in operational risk management practices.

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

The path of globalization has led to the integration of banking services in a number of ways that were unthinkable a several decades ago. The expansion, market integration and regulation, banks from country to country have created governance and economic framework that is complicates operations (Busch, 2009). The World Trade Organization (WTO) has been instrumental in lowering market and trade barriers, which have enabled financial institutions to better, meet the requirements of their depositors, customers, and clients (Busch, 2009).

According to Vardy (2015), the general perception of banks is that they avoid taking risks, although this perception is not always accurate. As a result, banks mistakenly put themselves in situations where they are vulnerable to a variety of financial hazards, the most significant of which is operational risk. These banks also face a dynamic regulatory and risk management landscape, as well as increasing customer demands and non-traditional banking automation technologies (Coetzee, 2016). These phenomena may be explained by variations in depositor habits. According to Ernst & Young (2012), these developments, as well as the uncertainties that arise from them, might have a major impact on the income and operating expenses of banks.

An operation risk is regarded internal if the financial institution can take measures to mitigate it, and external if it results from outside forces such as natural catastrophes, security breaches, or political risk (Hull, 2015). Financial organizations are constantly

exposed to operational risk occurrences, which make up a significant portion of the total risk exposure of a bank. When compared to other forms of financial risk, such as the possibility of a loss, operational risk is seen as a pure risk since it always ends in a loss for the bank (Rajendran, 2012). According to Ferreira (2015), the downfall of a number of banks and other types of financial organizations may be traced back to an inability to properly mitigate and manage operational risk during previous instances of operational risk.

This research is predicated on the fraud triangle hypothesis as well as the notion of differential association. The idea of fraud is based on a triangle that consists of three separate parts of deception: perceived pressure or motivations, perceived opportunity, and rationalization (Chiezey & Onu, 2013). The differential association hypothesis proposed by Sutherland (1949) asserts that criminal behavior may be learnt, just like any other topic.

The percentage of people who have been victims of economic crime has increased from 52% in 2019 to 61% in 2020, which is 25% more than the average for the whole world (PWC, 2021). Due to inefficiencies in operations management techniques and a general lack of integrity on the part of staff, Kenya has the largest number of instances of fraud and also has the highest prevalence of the problem. Commercial banks make up 66% of the country's victims. According to PWC (2021), Kenya is placed third with 61% incidences of fraud, behind South Africa with 69% and France with 68%; Zambia and Kenya are tied for third place, while Nigeria was ranked fourth.

1.1.1 Operational Risk Management Practices

Rapid growth is being seen in operational risk within the banking sector, yet most institutions have only lately become aware of this subset of risk. It has a significant relationship to the bank's internal policies as well as processes. It is feasible, as stated by Toroitich (2018), for operational risks to cause more damage to a bank than credit losses. The Basel Committee (2003) defines operational risk as the possibility of a loss due to malfunctioning systems, unforeseeable external events, inadequate internal processes, or human mistake. Given the ubiquitous nature of operational risk, the objective is to bring it under manageable control. Businesses need to look at their operations and their goals from every possible viewpoint when analyzing risk and developing strategies to reduce it. The purpose of operational risk management (ORM) is to lessen the impact of potential threats by identifying them, assessing them, assigning a monetary value to them, developing plans to minimize their likelihood and impact, putting those plans into action, monitoring them, and reporting on them (Toroitich 2018).

Risks associated with processing errors may be replaced by risks related with system failure when increasing reliance is placed on globally networked systems and automated technology is used. The expansion of international trade and e-commerce introduces new opportunities for risk, including the possibility of fraud on both the company's internal and external levels as well as problems with the system's overall security. Due to a rise in the number of banks doing high-volume service, it is crucial that they have robust internal controls and backup mechanisms in place (Lyambiko, 2015). It is feasible, as stated by the Credit-Suisse Group, to manage a bank's exposure to market and credit risk via the use of risk mitigation methods (2001). These methods may, however, introduce new

forms of risk, such as operational hazards. This group classified operational risks as follows: organizational risks; process risks; technological risks; human risks; and external risks. Another way to learn about ORM is to classify operational risks into several groups, such as those related to people, technology, and regulations. Because of the potential for operational risk, a financial institution must put in place a comprehensive risk management system that is made up of multiple components. These phases consist of recognizing the risk, quantifying the risk to the greatest degree feasible, and then selecting the most appropriate strategy to implement in order to mitigate the risk (Montgomery 2013)

1.1.2 Bank Fraud

A company's ability to continue business as usual and its relationships with external stakeholders, such as customers, suppliers, financiers, and business partners, may be jeopardized by fraud, which can also result in significant monetary losses. The banking industry occupies a significant place in the country's overall monetary structure and is an essential component in the expansion of an economy's overall scope (Ngalyuka 2013). Bank fraud involves the use of computers, the Internet, devices connected to the Internet, and services provided by the Internet in order to deceive individuals or organizations. Phishing, social engineering, and virus assaults are all examples of illicit computer actions that are associated with bank fraud (Ogechukwu 2013). Bank fraud is any purposeful conduct with the goal to manipulate financial statements for personal advantage (Mohammad 2015). The manipulation, fabrication, or change of records, documents, or numbers; misappropriation of assets records; records or documents that are missing certain transactions; misrepresentation of facts; a recording that is not supported

by solid fact; and a misunderstanding of how to apply the accounting rules are all examples of fraud. According to the findings of Malmi, Zainol, and Nelson (2012), environments in which quality management systems are inadequate and information technology is prevalent are more hospitable to fraudulent activity. The rising use of the internet by institutions based on information technology has led to an increased risk of fraud, which may result in significant financial loss.

General ledger fraud, identity theft, account takeover, and working with criminals outside the bank are some of the most common methods for committing bank fraud, as stated by Leuchtner (2011). Bank fraud was defined by Apoorva and Juhi, 2007 as any fraudulent activity that results in an unfair benefit at the price of monetary loss to a bank. There are several instances of bank fraud in which employees have a role, either as primary criminals or as facilitators working with other actors. They achieve this by disobeying established protocols, whether they did it alone or with the assistance of others. There is widespread agreement among corporations, senior bank officials, government officials, and powerful politicians to cheat financial institutions by bending or ignoring laws and regulations and ignoring generally accepted banking practices. Most bank fraud involving forgeries or manipulations of checks, drafts, or other instruments originates from sources outside the bank itself. Kamande (2018) argues that theft in banks may be quantified by tracking fraud rates, sums stolen, and trends over time. Both the frequency and magnitude of fraud will be taken into account in this analysis.

1.1.3 Commercial Banks in Kenya

Commercial banks (CBs) play a crucial role in the promotion of economic growth since they are responsible for directing money from areas with abundance to regions with a deficit for the purpose of investment. According to Yakubu and Affoi's (2014) research, there seems to be a significant connection between the function of CBs and the process of development. CBs, as defined by Machiraju (2008), are a specific subset of banks whose major function is to collect deposits, provide credit and account checking services, and distribute various types of financial goods to individuals and small enterprises. Certificates of deposit and savings accounts are two such items. The Kenya Bankers Association (KBA), which acts as an advocate for the interests of the banking industry, has brought the banks in Kenya together under one umbrella. The KBA acts as a venue to discuss problems that are relevant to its members. It was established as a cooperative initiative by the banking sector to advance its common interests and advance the sector's common goals. CBs and non-banking financial organizations both offer retail and corporate banking services, which reduce chances for investment in the banking business, according to the KBA's annual report (2021).

Companies Act, Banking Act and Central Bank of Kenya (CBK) Act stated prudential criteria provides the basis for and guides the development and operation of Kenya's banking sector. In addition to devising and executing monetary policy, the CBK is responsible for fostering liquidity, solvency, and the efficient operation of the financial system. There were 39 commercial banks licensed by the CBK as at the end of the fiscal year on June30, 2022. A bank's very nature makes it vulnerable to operational risks; these threats may have an effect on the bank's reputation, which is tied to its reliability and

success (Romnova & Kudinska, 2020). Establishing who the primary stakeholders of a bank are and prioritizing tasks in accordance with these stakeholders' characteristics, requirements, perceptions, risk tolerance, and financial behavior is the most significant work that a bank must do. According to Kanu and Okoroafor (2013), more than eighty percent of organizations throughout the world consider their customers to be the most significant group of stakeholders. Depositors are the most significant external stakeholders for institutions that protect deposits, including retail banks, commercial banks, and savings banks, since depositors are the organizations' primary clients.

1.2 Research Problem

Financial stability and performance of financial institutions are both put at risk by operational risk. A commercial bank's reserves, expenses, and stock price may fluctuate if operational risk wasn't properly managed (BCBS, 2020). It's the drop you take when your own people, systems, and procedures fall short or when something beyond your control causes a problem. Losses suffered as a result of things like internal and external fraud, poor human resources (HR) policies, unsafe working conditions, damaged physical assets, disrupted operations, botched product launches, botched product deliveries and botched process management. As illustrated by Hess (2011), Andersen et al. (2012), and Robertson, failure to systematically handle operational risk may lead to fraudulent activity and inconsistent performance, decreased profitability for the stakeholders, and an influence on the revenues and net worth of banks (2011). ORM deficiencies may result in an increased risk of being exposed to fraudulent operations, which in turn can raise a bank's vulnerability to reputational and strategic concerns. If a proper risk management system is not maintained, the bank runs the risk of severe fraud, defalcation (For instance,

when a worker takes money that belongs to the firm without permission), and other operational losses.

The 2008 financial crisis and the collapse of many large corporations including Enron, WorldCom, and Bank of credit and commerce international (BCCI) have led to an increase in the number of inquiries into the causes of these disasters (Aduda, Chogii & Magutu 2013). According to Chernobai, Jorion, and Yu (2011), a number of high-profile losses have been connected to operational risk. One example of this is the $7.2 billion loss that Société Générale experienced in 2008, which was partly attributable to the lack of internal controls and mismanaged operational risks. The practice of fraud dates back to the beginning of time and has evolved into many different guises throughout the course of history. Fraud committed using computers has increased along with the development of the financial sector. This growth has been made possible by advances in technology and the proliferation of Internet usage. According to Cressey's model of fraud from 1973, there must be a confluence of three conditions for fraudulent activity to take place: opportunity, pressure, and rationalization. Deloitte found that in 2012, East African banks lost a total of Sh4.1 billion ($48.3 million) due to fraud, with more than half of that amount coming from Kenyan banks due to the ease with which technology promotes fraud.

The findings of Altunbas et al. (2018) indicate that it is more probable for banks to engage in unethical behavior when their CEOs have held their positions for a longer period of time. The research carried out by Eshraghi and colleagues (2015) on regulatory measures taken against US banks demonstrates that board monitoring and advising are

both useful tools for minimizing the risk of improper behavior on the part of financial institutions. Fich and Shivdasani (2007) investigate whether or not enterprises with external directors incur reputational consequences if the companies on which such directors serve are suspected of financial malfeasance. Researchers Schnittker et al. (2017) found that a rise in risk-taking in the UK mortgage market follows a negative bank capital shock by using provisions for misbehavior costs as an instrumental variable to isolate the influence of the shock on bank behavior. There is a possibility that business and financial cycles are interwoven with operational risk. Carrivick and Cope (2013) and Hess (2011) investigate the effects that the Great Banking Crisis had on the financial industry's operational risk losses. Abdymomunov et al. (2017) give more evidence that there is a connection between operational losses in US banks and the circumstances of the macroeconomic environment.

Oreku (2013) contends that the banking sector is still grappling with how to effectively combat fraud as a result of the social stigma that is associated with the disclosure of private financial information. Fraud committed using computers has mostly supplanted more conventional methods of stealing from banks, and Kenyan institutions have not been exempt from this trend. Zagaris (2010) determined the influence that computerization has had on the increase of fraud throughout the world, while Gasaioro (2016) investigated how fraud is handled in financial institutions. Additional context on the challenges posed to the banking sector by postmodernism and electronic transactions may be found in research presented in Onyango (2014). There is a noteworthy lack of easily available written literature in Kenya on topics related to fraud in the country's commercial banks.

This is as a result of the fact that there has been no study conducted on the impact that operational risks management techniques have on the rate of fraud that occurs in Kenya's commercial banks. Therefore, this research is to look at the connection between bank fraud in Kenyan businesses and operational risks management techniques. This study aims to address the following research question: How do operational risks management methods relate to commercial bank fraud in Kenya?

1.3 Research Objectives

The general objective of the study is to establish the effect of operations risks management practices on fraud among commercial bank in Kenya.

The specific objectives of the study are:

i. To determine the effect of risk identification of operational risk management practice on fraud among commercial banks in Kenya

ii. To determine the effect of risk assessment of operational risk management practice on fraud among commercial banks in Kenya

iii. To evaluate the effect of measurement and mitigation of operational risk management practice on fraud among commercial banks in Kenya

1.4 Value of the Study

The day-to-day operations of the bank must be managed to reduce operational risks by ensuring they are carried out in accordance with predetermined plans. Industry examples that stand to gain greatly from this study's findings include the financial industry leaders,

such as top bank executives, since it provides direction on the process for monitoring and assessing operational risk. Commercial bank employees who deal with ORMon a regular basis will be able to learn from the study's findings and adjust their practices accordingly.

There has not yet been a publication of guidance on ORM for Kenya's local banks by Kenya's regulatory bodies. The Central Bank of Kenya's Department of Banking Supervision will benefit from the knowledge that this research offers them. The foundation for the conduct of more research on the topic will consist of academics that have an interest in the topic under investigation. The current pool of knowledge in the subject of finance will get fresh contributions as a result of this study.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter provides a survey of the relevant literature as well as a number of different ideas on the topic that is being studied that have been provided by a number of different researchers, academics, analysts, theorists, and writers. I have taken elements from a variety of sources that are pertinent to the topic and goals of the research, and I have organized them into a coherent whole.

2.2 Theoretical Review

In order to get insight into information systems as well as fraud, three different ideas have been examined. The theory of the fraud triangle, the theory of differential association, and the operation risk theory are the names of these hypotheses.

2.2.1 Fraud Triangle Theory

In 1973, criminologist Cressey first proposed the hypothesis based on his study of 200 convicted embezzlers (trust violators) housed in different jails around the Midwest of the United States. Trusted people, he said, cross the line into trust breakers when they see themselves in a circumstance where they have a private financial issue that can be remedied by discreetly abusing their position of financial trust (Cressey, 1973). The fraud triangle is a popular tool in the auditing industry that summarizes the conditions that might foster fraudulent behavior. The fraud triangle outlines the ways in which opportunity, motive, and justification may raise the likelihood of fraudulent behavior.

For a number of years, Cresset's Fraud Triangle has been put up as an explanation for the characteristics of people who commit fraud. According to Dorminey (2012), while the theory is an essential component of a model for determining the likelihood of fraud, an entire audit risk assessment strategy includes it as just one component. Wells (2005) posits that, the fraud triangle hypothesis has been roundly condemned for its use in areas such as the prevention, detection, and punishment of trust breach crimes. Day (2010) has also said that they concur with the viewpoint that the fraud theory triangle has not showed any signs of being beneficial in the battle against fraud. The fact that this model identifies antecedents that may be present in a significant proportion of situations that do not end in fraudulent activity is an evident criticism of the model. As a result, the fraud triangle is not a predictive model; rather, it is a descriptive model that functions most effectively when used to post hoc investigations (Day, 2010).

When a company's current or projected financial state and resilience are endangered by inadequate or failing internal processes or systems, human error or misbehavior, or adverse external events, the result is operational risk (Ekechi 2019). For instance, a possible operational risk is bank fraud. ORM flaws may make a company vulnerable to the fraud triangle's three prongs: pressure, opportunity, and rationalization. This, in turn, can raise a bank's exposure to reputational and strategic risks. In the event that a proper risk management system is not maintained, the bank runs the danger of being subject to major instances of fraud, defalcation (such as the theft of money by a worker), and other types of operational losses.

2.2.2 Theory of Differential Association

Differential association theory, which was developed by Sutherland and Cressey in 1974, places an emphasis on the process of socialization and claims that criminal behavior is learnt via close personal relationships. Sutherland's thesis is not only one of the most influential criminological theories ever proposed, but it is also the foundational theory that served as the basis for the development of a number of additional ideas. One of the theories of crime that has been put through the most rigorous testing and has received the greatest support is differential association (see Pratt et al., 2010).

According to Sutherland (1949), criminal behavior may be taught in the same way that other subjects can. He was of the opinion that criminal activity only took place in the presence of other people and as part of a coordinated communication process; hence, he felt that criminal activity could not take place in the absence of the assistance of other individuals. Because criminal conduct is the result of competing values, it is caused when a person is presented with more meanings that are advantageous to breaking the law than they are with definitions that are unfavorable to doing so. The hypothesis has been called into question due to the fact that it does not take into consideration individual variations. Differential association theory may not be able to explain some results brought about by the interaction of a person's personality characteristics and their environment (Matsueda 2010).

White-collar workers' propensity toward criminal behavior may be understood via the lens of differential association, a theory of criminal learning. This theory can be found under the broader heading of the learning theory of crime. The method by which criminal

conduct is learnt, as well as the substance that a person learns from the process, are the two primary postulates of this theory (Sutherland, 1947). The differential association theory is an attempt to provide evidence that criminal behavior is acquired knowledge. It does this by focusing on the relationships between criminals. According to Dorminey et al.'s (2020) argument, criminal conduct may be picked up via contact and affiliation with other members of the same kind of organizations. Exposure to and learning from those who share one's criminal inclinations increases the likelihood that an individual may participate in illegal action.

2.3 Operational Risk Management Practices

Risk Management is an integral part of a business's or organizations larger context, which is geared at identifying and quantifying prospective risk scenarios as well as devising the strategies essential for controlling them. Typically, this is carried out within the context of a business or other formal organization. The goal of risk management is to enhance shareholder value by limiting the negative effects of the various potential dangers a company confronts, according to Hopkin (2010) and the indictors they considered risk identification, risk assessment, risk measurement, mitigation and reporting.

For an ORM system to be effective, risk identification must be a priority. Internal and external variables are taken into account as part of an efficient risk identification process. This enables the financial institution to have a deeper comprehension of its risk profile and more precisely direct its risk management resources and strategies (Soltani, 2014). In order to regulate and mitigate possible hazards, financial institutions need to be aware of such risks. Every financial institution that extends credit has its own set of standards and

control mechanisms to help it detect and mitigate possible risks. A financial institution is able to take preventative steps in the face of risks by first identifying the origins of such risks and the factors that contribute to those risks (Singleton & Singleton2010).

During a risk assessment, a bank evaluates the processes that are fundamental to its operations against a database of possible risks and vulnerabilities, taking into account the potential effect that these factors may have. Its purpose is to detect operational risk and make judgments that will either include taking the risk or staying away from it. Every firm is subject to a wide variety of hazards, which need to be evaluated in an efficient manner (Kingsley 2012). The primary goal of doing a risk assessment is to single out important operational risks and then, ultimately, to evaluate those risks. The majority of the time, they are administered in the form of surveys, workshops, and interviews. The qualitative assessments that were gathered are helpful in determining the severity of the loss and in rating hazards so that important concerns may be identified. The risk portfolio may be displayed in the form of a risk map or matrix, which details the organization's relative advantages, disadvantages, opportunities, and threats.

The process of an organization putting into place steps to reduce or get rid of hazards that are deemed undesirable is referred to as risk mitigation. To intellectually minimize the degree of effect and the likelihood of recurrence of risks deemed undesirable by the banking industry, mitigating measures are developed (Birindell & Ferretti 2017). Risk reduction is the process of reducing the likelihood of negative outcomes, which is why financial institutions do not accept or undertake all risks. If a bank's risk margin for its operations is smaller than the projected risk cost of accepting all of the risk, then the bank

should avoid taking the risk (Yegon 2015). The organization as a whole is being monitored for its risk management, and any required modifications are being made. Monitoring may be carried out in one of three ways: via continuous management operations; separate assessments; or all of these. In today's world, financial institutions are under increasing technological pressure to automate their service delivery, and whether newly implemented or old, their systems are constantly exposed to threats such as hacking, denial of service attacks, and the possibility that they will be exploited by third parties (Adeyemo, 2012).

2.4 Determinants of Banks Fraud

The degrees of fraud are influenced not only by factors that are internal to the banking business but also by those that are external to it and the surrounding economy. The internal environment encompasses both the strong points and the problematic areas of specific financial institutions. However, the external environment not only causes threats but also offers the banking industry with a variety of opportunities. By capitalizing on the prospects, banks in the business have the potential to grow their profitability as well as their market share and client base; nevertheless, doing so may accidentally make the danger of fraud more widespread.

2.4.1 Technology Environment

New product and service creation, research, and the implementation of cutting-edge approaches in customer service would not be possible in the banking business without the omnipresent presence of information technology. The storing, processing, and analyzing of financial data has been completely disrupted by technological advancements. At the

same time, it has contributed to an improvement in the quality of financial services, capacities related to risk management, as well as a decrease in banking expenses and an increase in the lending capacity of banks (Wilson et al., 2010). With the expansion of globalization, information and ideas between foreign banks may be exchanged with greater ease (Claessens and Horen, 2008). This research will focus on the impact that information technology plays in the initiation, maintenance, and discovery of financial fraud.

When comparing local and foreign banks, one of the most striking differences is likely to be in how each makes use of ICT. Furst et al. (2002) observed that internet banking was more popular among financial institutions that were part of a bank holding company (international banks and branches), were situated in a large city, and had relatively high fixed operational expenses compared to operating revenue. As a result, it has become clear that factors such as bank size, population density, and proximity to major employers are all very consequential in determining whether or not a certain population adopts online banking (Wilson et al., 2010).

2.4.2 The Socio-Cultural Environment

Age, gender, education, unemployment, and a broad range of social values and ethics are only some of the demographic and socioeconomic indicators that define the sociocultural context. In the world of corporate banking, corruption is a widespread societal issue (Bakre, 2007; Transparency International, 2009), and this problem has ramifications for the cultural norms that govern business conduct (Zahra, Priem, & Rasheed, 2007). When

taking into account the influence that financial systems have on the growth of an economy, it is very essential that these systems function well.

Corruption is one of the primary reasons why banking systems in poor nations do not always function effectively. The lack of adequate legislation, prudential guidelines, an efficient and fair legal system, and other essential institutions exacerbates the situation. Corrupt practices tend to decline, however, when courts are given more independence and law enforcement is strengthened (Barth et al., 2009). According to the findings of Barth (2009), more competition and information exchange among financial institutions helps to minimize instances of fraudulent bank lending practices. It was also discovered that there was a lower incidence of corrupt lending practices in businesses that were controlled by governments or other countries, as well as in banks whose forms of ownership were private and foreign.

2.4.3 Internal controls

A robust system of internal controls is often the first line of defense that a business may use to prevent fraud from occurring inside its ranks. Though a lack of internal controls is not a guarantee of fraud, it does raise the risk that it will occur. Careless inventory management, a lack of documentation to back up cash transactions, an improper allocation of responsibilities, ineffective or outdated accounting software, and a lack of third-party verification are all signs of a lack of internal controls (Doyle et al., 2007; Porter, 2003).

According to Lokanan (2014) auditing has taken on an increasingly prominent part in the prevention of fraudulent activity. The audit function significantly affects the typical fraud

loss and it seemed to show that audited organizations had incurred less severe fraud losses in comparison to those that had not been audited. The employment of managerial supervision as a deterrence strategy may be quite successful. However, the concept that someone is monitoring and watching you helps inhibit fraudulent activity to some degree since it raises the impression of the likelihood of discovery. Therefore, the primary functions of internal audits are those of detection and prevention (Huber, 2017).

2.5 Empirical Review and Knowledge Gaps

The financial institution of today is facing a variety of issues, some of which are related to finances while others are not; the majority of these issues are a direct consequence of inefficient operational methods. A robust system of operations is the cure for the difficulties that have been plaguing the banking sector. Many banks have collapsed as a result of a lack of adequate controls (Tunji, 2013). According to observations made by Hartman (2014), the loopholes that dishonest individuals often look for before engaging in unethical behavior are found in inadequate systems of operations control. According to Hartman (2014), the banking sector has seen a significant number of losses as a result of inadequate ORM. Therefore, financial institutions must put in place stringent protocols if they want to eradicate or considerably decrease unethical activity inside the organization and in the wider community.

The effectiveness of internal control systems in the Nigerian banking industry in preventing fraud was assessed by Ajala, Amuda, and Arulogun (2013). Five commercial banks' audited public financial accounts were used to compile this data, which was then evaluated using the product moment correlation coefficient and regression. After

implementing an efficient internal control system, they find that fraud against Nigerian banks has dropped significantly. They concluded that the ineffectiveness of internal control mechanisms in Nigerian banks was due to inadequate corporate governance.

Research on banking fraud schemes and potential prevention measures was undertaken by Zuraidah, Mohd, and Yusarina (2015). The management structure of Malaysian banks was studied in depth, including the roles of branch managers and assistants' managers in the processing of home mortgages and car hire purchase agreements. The results of the research demonstrate that fraudsters often possess intimate knowledge of the industry they target and use this expertise during the commission of the scam. In light of the fact that fraudsters will forever be inventing new methods of deceiving financial institutions, the industry has accepted the reality that fraud risk cannot be eliminated entirely. Therefore, they advocated for a stronger emphasis on the essential tasks of financial institution staffs in order to make their responsibilities more evident in the prevention of fraud.

According to research conducted by Koomson (2011) on ORM in the Ghanaian banking sector, this field is only getting its feet wet across the country's numerous financial institutions. However, banks have only recently realized that their day-to-day operations are riddled with risks that, if not successfully handled, may result in major losses (loss of clients, money, and reputation). In response to increasing levels of competition, the Bank of Ghana has issued a directive requiring all financial institutions in the nation to implement operational risk management. This directive is in accordance with the recommendation made by Basel II to allot some capital to compensate for operational

risks as they become apparent. Due to the fact that the board of directors and the rest of the financial institution are required to participate in operational risk management, the industry as a whole is consolidating around a common set of strategies and goals.

Namanda (2010) produced an essay titled "The Role of ORM Strategies in Combating Fraud in Financial Institutions" that used Standard Chartered Bank in Uganda as a case study. The study's main goal was to analyze Standard Chartered Bank's ORMP with a view toward identifying its contribution to the prevention and detection of fraud at other financial institutions. In order to gather data from a number of different departments, including Operations, Credit, risk/Audit, and Treasury, a research methodology known as cross sectional was used. The workers of Standard Chartered bank served as the pool of potential responders, and a method called purposeful sampling was employed to pick fifty of them. The key findings indicated that fraud risk might be mitigated by the use of ORM strategies.

To examine the prevalence of fraud and the motivations of fraudsters, Akelola (2012) research makes use of a theoretical framework based on the Fraud Triangle. There are sixty survey respondents and seventeen semi-structured interviews used to compile this mixed-methods qualitative and quantitative research on fraud prevention in the banking business. Managers from auditing, fraud detection, security, and related fields are included in this study's sample. The research concludes that fraud is widespread across the Kenyan banking industry, despite the fact that individual fraud cases tend to be small and straightforward. Conventional methods were utilized to identify and prevent fraud in the industry, and these methods were consistent with those used elsewhere. The fraud

triangle was able to accurately forecast the patterns of fraud that were stated by respondents thanks to its use. This study, in contrast to others that have concentrated on either individuals or their environments, adopts a theoretical and conceptual framework that considers fraud as a whole.

Sang (2012) delves at the elements that influence the fraud control strategies used by Kenya's commercial banks. This descriptive research used a questionnaire to collect its data. In order to analyze the data, both descriptive and inferential statistics were utilized. Lack of commitment to the dual control concept was shown to be a significant factor reducing the efficacy of internal control measures. Another factor was a shortage of adequate time to carry out the numerous periodic tests with enthusiasm. Compliance with fraud mitigation techniques was to be strictly enforced, and staffing numbers were to be increased in key areas, among other recommended steps to deter fraud.

Wanjiru (2011) conducted a case study at Equity Bank of Kenya Limited with the purpose of obtaining in-depth knowledge about the tactical solutions to growing fraud-related concerns. According to the findings of the research, fraud is a sensitive topic, and consumers have an enormous fear of becoming a victim of fraud. Furthermore, fraud has a negative influence on the profitability of banks, as the cash lost due to fraud would have otherwise been spent to stimulate development. According to the findings of the research, identity theft is the most significant threat posed by fraudulent activity. Passports, ID cards, and driver's licenses may all be readily forged by criminals due to the ease with which they can be reproduced. The study also found that check fraud is a common kind of

fraud, with the major cause being that customers with cheque books do not take enough safeguards to ensure that their books are kept in secure custody.

According to Muia (2016), inadequate ORM on the part of many insurance companies has resulted in the accumulation of many claims either from internal clients or eternal clients, which has consequently led to increased losses and poor financial performance for many corporate organizations. Insurance firms are in the business of mitigating risk, both for their policyholders and for the company themselves. This necessitates that they institutionalize risk management approaches across their organizational infrastructure, processes, and ethos. Insurance companies may more clearly see the value of using a risk management framework if they establish a link between risk management and financial results. No studies have been conducted in Kenya that analyzes how different ORM techniques affect the bottom line of insurance companies. By carrying out research on the topic at hand, the study attempted to close this knowledge gap. A descriptive method was used for this study's analysis. Each of the 47 active insurance companies in Kenya was surveyed as part of the research.

According to Mwanzia (2021), risk management typically results in increased financial performance for an organization. This is likely the case given that risk management and risk control enable an organization to save money. The study set out to answer the question of whether or not risk management can boost the overall financial performance of Kenya's commercial banks. The method of descriptive research was used throughout the course of the investigation. The gathering of secondary data, which extended over the span of five years from 2016 to 2020 and was assisted by secondary data sources in the

form of yearly Bank Supervision Reports, was carried out. The management of operational risk demonstrated a favorable correlation with financial performance, despite the fact that this correlation was small.

The impacts of risk management on the financial performance of banks in Kenya were evaluated in this study, which Okello, G. A. (2021) states spanned the years 2016-2020. The study aimed to accomplish the following four things. The goals of these analyses were to determine if credit risk was a significant factor in the financial performance of Kenyan banks, to determine whether market risk was a significant factor in that performance, and to determine whether liquidity risk was a significant factor in that performance. Throughout the course of the research, participants drew upon the insights of the Modern Portfolio Theory, the Transaction Cost Theory, and the Liquidity Preference Theory. Each of the 39 commercial banks in the nation was enumerated, and their data was culled from their financial statements and the CBK's annual supervisory reports. Market risk was the most detrimental to the overall financial performance of commercial banks, followed by operational risk, credit risk, market risk, and liquidity risk. Since commercial bank performance declined as all of these factors increased throughout the course of the research period, it is reasonable to conclude that any one of them may have caused the decline.

2.6 Conceptual Framework

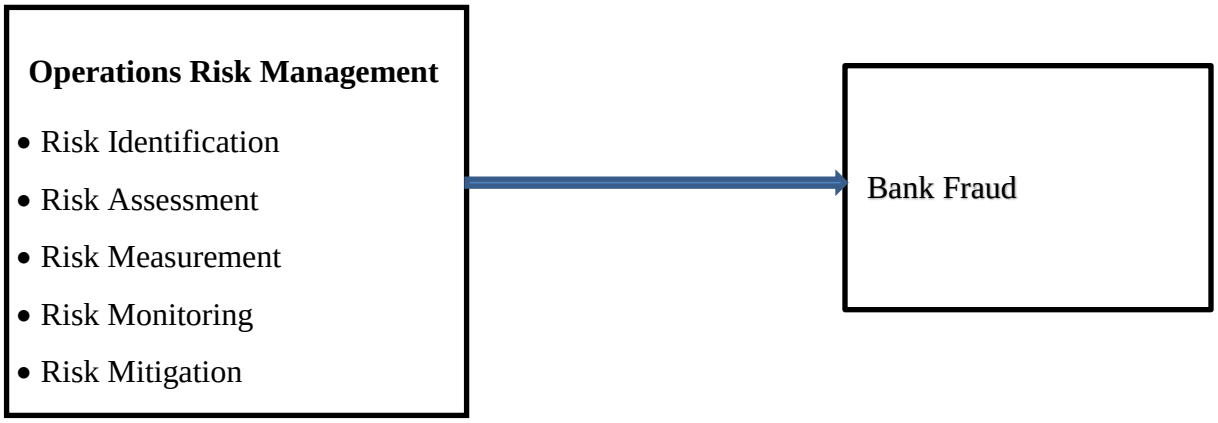
The objective of a conceptual framework, as defined by Cooper and Morgan (2008), is to aid researchers in correctly identifying the issue they are examining, developing appropriate research questions, and accessing appropriate sources of information. A

conceptual framework is used at the beginning of the majority of academic research since it assists the researcher in elucidating both his research topic and his goals.

A conceptual framework has been created by reviewing the current literature, together with theoretical and empirical studies. This framework considers many research needs and pinpoints places where operations risk management could have an impact on fraud. Operations risk management is the independent variable and bank fraud is the dependent variable in the present research. The whole architecture is shown graphically in Figure 2.1. The conceptual diagram delineates between dependent and independent variables.

Figure 2.1: The Conceptual Model

Independent Variable **Dependent Variable**



Source: Author 2023

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

An outline of the research methods that was use employed is provided in this section. First and foremost, it focuses on the study's layout, next on the data analysis methodologies, and lastly on the data collection and presentation strategies that was used in this investigation.

3.2 Research Design

A descriptive, cross-sectional approach was used for this study. This descriptive cross-sectional study approach (Creswell, 2012) allows for clearer communication of information on the nature and context of an event. The researcher opted for a descriptive cross-sectional survey design for the purposes of this study. This approach is valid because it allows for a comparative analysis of a set of events, circumstances, and people, communities, or populations through time (Chandran, 2004). The investigations that were conducted by organizations at the same moment in time make this design appropriate.

3.3 Population of the Study

Given the goals of the study, the pool from which the sample was drawn included all Kenyan commercial banks. There are a total of 39 commercial banks in this association as of the end of 2022 (Appendix II). All commercial banks as of December 31st, 2022 (CBK Report, 2022) that have been in business for at least five years were included in the sample. The study was conducted via the use of a census survey in Kenya because of the country's high concentration of commercial banking institutions.

3.4 Data Collection

In order to achieve the goals of this investigation, primary data was employed in the data gathering and analysis procedures. Primary data on ORM and bank fraud was gathered via the use of questionnaires due to the benefits questionnaires provide over other methods of data collecting, such as lower costs. Questionnaires were the major method of data collection. There are three parts to the questionnaire's format. The first part included some standard profile questions and background data. A Likert scale was used in the second section of the survey to gauge respondents' level of agreement with statements about operational risk management, and in the third section, the survey used Appendix I to learn about the current state of bank fraud prevention processes utilized by commercial banks in Kenya. Risk management, human resources, and finance department heads all provided replies.

3.5 Data Analysis

The information that was gathered was modified to ensure that it is accurate, uniform, consistent, and comprehensive. Before the final analysis was carried out, a preliminary arrangement was developed in order to make the coding and tabulation processes easier. The qualitative data was evaluated by first categorizing, and then clustering, the many theme components obtained, to offer responses to the study objectives. That was done so that the study's results could be looked at more thoroughly. Descriptive statistics were used in order to gather relevant percentages, frequency counts, modes, median, and mean values from quantitative research in order to analyze and understand the findings. The purpose of this was to collect useful data. An additional linear regression was utilized alongside this method for data analysis throughout the investigation.

The use of correlation analysis allowed for the characterization of the degree to which one variable is associated to the other variable. It is expected that there is a linear connection if there is any relationship at all. As part of this investigation, we determined the coefficient of correlation (r), as well as the coefficient of determination (r2), in order to have a better understanding of the dynamics and breadth of the connection. The correlation coefficient was used in order to provide an assessment about the degree to which ORM and fraud are associated with one another. The data, together with the variables and the values, were entered into SPSS version 22 for analysis so that the correlation coefficients could be computed. Also included in this analysis were the variables.

In order to do an analysis on the collected data, the researcher employed a technique called multiple regressions. When a researcher is interested in determining whether or not a certain independent variable can accurately predict a specific dependent variable, they will turn to regression analysis. The goal of multiple regressions is to establish whether or not a set of factors can, on their own, accurately predict a certain dependent variable i.e. computer fraud, payment fraud and credit card fraud.

3.5.1 Diagnostic Tests

Diagnostic procedures such as checking for normality, multicollinearity, homogeneity, and autocorrelation will be performed to ascertain the model's viability. Under normality, the residual of the dependent variable is assumed to follow a normal distribution and to cluster around the mean. Either the Shapiro-Wilk test or the Kolmogorov-Smirnov test was used in order to attain this goal. In the case that one of the variables does not have a

normal distribution, the logarithmic adjustment technique was used to alter the value of the variable in question. The autocorrelation coefficient is a statistic used to evaluate the persistence of a time series' connection with its own delayed value. The Durbin-Watson statistic was used in the process of evaluating the results of this test. In the case that the supposition is shown to be incorrect, the model will make use of the robust standard errors (Khan, 2008).

The phenomenon known as multicollinearity occurs when a large number of independent variables are fully or almost perfectly associated with one another. Tolerance levels and Variance Inflation Factors (VIF) were included into the analysis. Every multicollinear variable was eliminated, and in its place, a fresh measurement of the variable that demonstrates collinearity was carried out. A statistical test known as heteroskedasticity is used to examine whether or not the error variance in a regression can be attributable to the variables that are being controlled by the researcher. It was analyzed with the help of the Levene test, and in order to fulfill the need for the homogeneity of variances assumption, robust standard errors were used (Burns & Burns, 2008).

3.5.2 Analytical Model

An econometric model was used for the regression analysis that was done down below.

$$Y= \beta 0 + \beta 1\ X1 + \beta 2X2 + \beta 3X3 + \beta 4X4 + \beta 5X5 + \alpha$$

Where; Y= Bank Fraud (Likert Scale)

X1 = Operational Risk Identification (Likert Scale)

X2 = Operational Risk Assessment (Likert Scale)

X3 = Operational Risk Measurement (Likert Scale)

X4 = Operational Risk Monitoring (Likert Scale)

X5 = Operational Risk Mitigation (Likert Scale)

3.5.3 Test of Significance

The explanatory capacities of the model, as well as the degree to which the data are compatible with the statistical model, are both assessed with the use of the coefficient of determination (R2). The relevance of the F statistic is investigated while attempting to ascertain the overall importance of the models. Analysis of variance (ANOVA) tests are used to examine whether or not certain variables are statistically significant throughout the process of deducing conclusions from an experiment's findings.

Table 3.1: Summary of Methodology

Objectives	Data Type	Purpose	Data Analysis
Evaluate the effect of risk identification of ORMP on fraud among CBK	Primary and Secondary Data	To investigate whether risk identification has any effect on fraud among CBK	Frequency Tables, Means, Percentages
Determine the impact that the risk assessment of ORMP has had on the incidence of fraud among CBK.	Primary Data and Secondary Data	Examine the role of risk assessment in preventing fraud in Kenya's commercial banks.	Frequency Tables, Means, Percentages

Evaluate the effect of measurement of ORMP on fraud among CBK	Primary Data and Secondary Data	To find out how measurement relate to fraud among CBK	Tables, Frequency, mean, correlation and regression
Determine the impact that the risk monitoring of ORMP has had on the incidence of fraud among CBK.	Primary Data and Secondary Data	Examine the role of monitoring in preventing fraud in Kenya's commercial banks.	Frequency Tables, Means, Percentages
Evaluate the effect of mitigation of ORMP on fraud among CBK	Primary Data and Secondary Data	To find out how mitigation relate to fraud among CBK	Tables, Frequency, mean, correlation and regression

CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

The major goal of this study was to examine the prevalence of fraud in Kenya's commercial banks in relation to the handling of operational risks. This summary presents the study's findings after breaking them down into their component parts (data analysis, descriptive statistics, correlation analysis, regression analysis, results, and commentary). We used averages, standard deviations, percentages, frequency distributions, and correlation coefficients to illustrate the findings.

4.2 Data Presentation

Data was presented in the form of tables and graphs, where the averages and standard deviations were discussed.

4.2.1 Response Rate

It was planned that 39 Kenyan commercial banks will participate in the data gathering for this project. A total of 117 persons representing the demographic were asked to fill out the survey. The information was derived from the responses of these persons. Approximately 55% of respondents were able to fill out the data collection form correctly (Mugenda & Mugenda, 1999) and thereby meet the reporting requirements. Simply put, it met the criteria for a reportable form. The percentage of respondents that met all of the criteria for inclusion in the sample may be inferred from the data completion rates. Out of

a total of 117 questionnaires sent out, 82% (70) were filled out and returned for analysis. This rate of return was deemed enough for the research.

4.2.2 Demographic Information

This section deals with section of the questionnaire which sought to understand the background of the respondent. The first question was about the gender of the respondent.

Table 4.1: Gender

FACTOR	FREQUENCY	PERCENTAGE
Male	51	62
Female	31	38
TOTAL	**82**	**100**

Source: Research Findings (2023)

As seen in table 4.1, male respondents made up the majority of the sample, with 51 (62%) of the total, compared to just 31 (38%) female respondents. According to the findings, the majority of the people that participated in the survey were male.

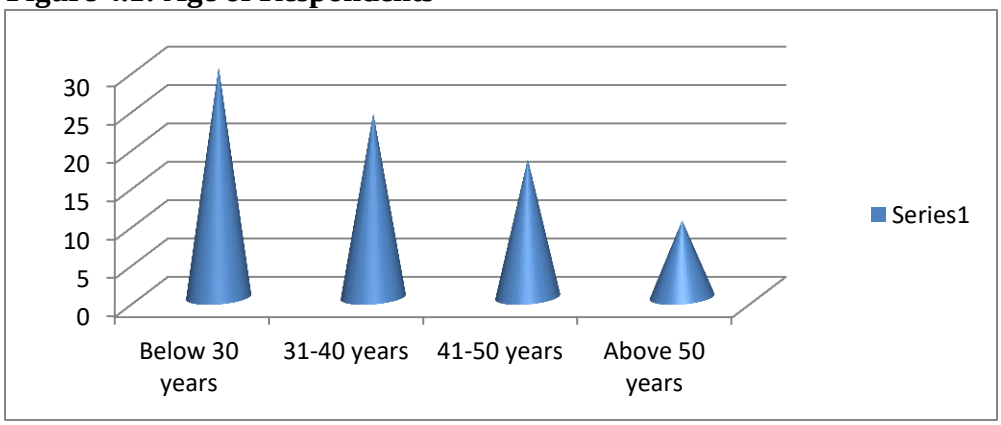
Table 4.2: Age of Respondents

FACTOR	FREQUENCY	PERCENTAGE
Below 30 years	30	37%
31-40 years	24	29%
41-50 years	18	22%
Above 50 years	10	12%
TOTAL	82	100%

Source: Research Findings (2023)

Table 4.2 shows that 37% of the participants below 30 years old. 29% were in the 31-40 year old range, 22% were in the 41–50 year old range and 12% were in the 50 plus year old range. These results suggest that the majority of responders were below 30 years.

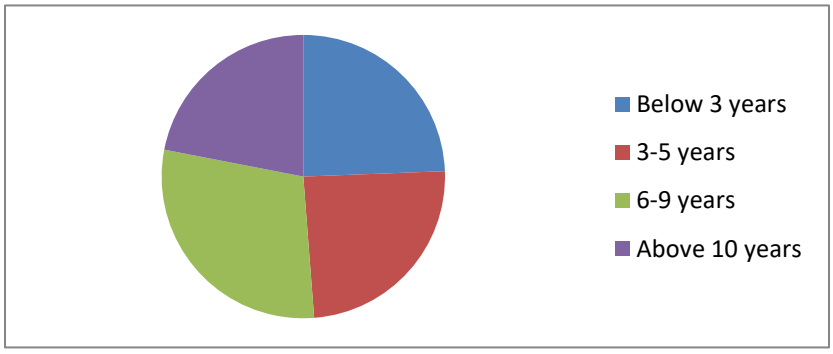
Figure 4.1: Age of Respondents



Source: Research Findings (2023)

From Figure 4.1 there was an indication that majority of the banks employees were below the age of 30 years and below, followed by the age group of between 31 to 40 years. Coming third was the age group of between 41 and 50 years. The banks who were above 50 years were minority.

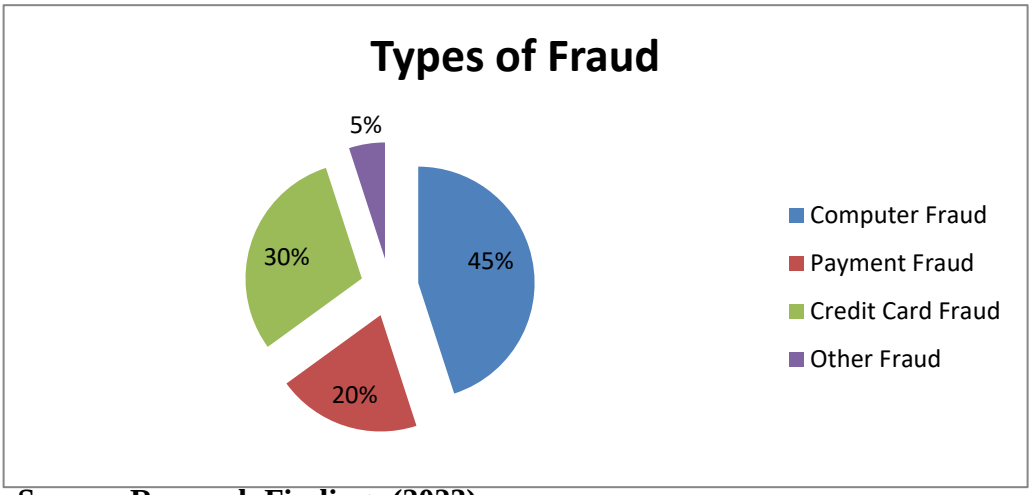
Figure 4.2: Years in Current Position



Source: Research Findings (2023)

According to Figure 4.2, the majority of bank workers have worked in their present job for between 6 and 9 years, with 3-5 years coming in second and less than 3 years coming in third while those who have worked in their roles for 10 years or more made up 22% of the workforce.

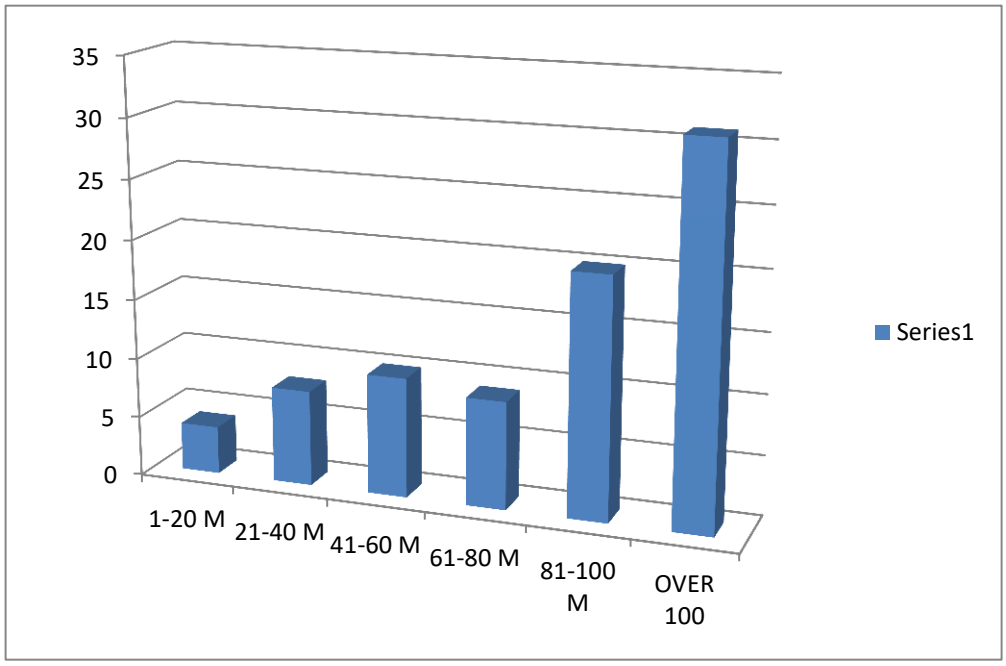
Figure 4.3: Types of Fraud



Source: Research Findings (2023)

Figure 4.3 indicates that majority of fraud cases were computer fraud at 45% followed by credit card fraud at 30%. Payment fraud was 30% while other type of fraud was at 5%.

Figure 4.4: Amount of Fraud



Source: Research Findings (2023)

From figure 4.4 most of the in the banks were in the tune of Kshs 100million as indicated by the respondents, followed by frauds between 81million to 100million. The rates of fraud for the small amounts of less than 20 million were few.

4.2.3 Operational Risk Management

Loss due to an internal process, people, or system failing, or to long-term events, is known as operational risk. According to the Basel Committee on Banking Supervision (2001), operational risk is defined as the potential for financial loss as a result of internal or external events that affect the whole organization. Acceptance, management, and reduction of risks may all be guided by a cycle or road map known as risk management (Cheng, Yip, & Yueng, 2012). Implementing procedures, rules, actions, and instruments

with the intent of managing risks and making them acceptable is what risk management is all about, according to Alhawari et al. (2012). The mission of risk management, according to the Institution of Risk Management (IRM), is to "enhance the probability of success while minimizing the probability of failure" for enterprises. It also covers risk management, which involves creating risk management methods to prevent risks, reduce their negative effects, and accept part or all of their repercussions.

Table 4.3: Operational Risk Management

	Mean	Std Dev
Across the board, the bank has an agreement on how to handle operational risk.	4.3846	1.4558
In the bank, there is a good system in place for comprehending the several hazards that are there.	4.4103	1.5245
The ORM responsibility has been outlined in detail and is understood by all employees within the bank.	4.4872	1.4011
The bank as a whole has a crystal clear understanding of who is responsible for what with regard to operational risk management.	4.3333	1.5349
The bank provides its customers with a comprehensive set of rules and recommendations to follow in order to effectively manage operational risk.	4.5385	1.6506

Source: Research Findings (2023)

Based on the data shown in the table above, it seems that most financial institutions have implemented ORM procedures. The highest mean was 4.5385, the bank provides its customers with a comprehensive set of rules and recommendations to follow in order to effectively manage operational risk. The lowest was 4.3333, i.e. the bank as a whole has a

crystal clear understanding of who is responsible for what with regard to operational risk management

4.3 Diagnostic Tests

On the basis of the information acquired, diagnostic tests were carried out. It was determined whether or not there was a problem by doing tests such the Normality test, Multi-collinearity analysis, and Homoscedasticity analysis. The purpose of carrying out normality tests is to establish whether or not the sample data being used originates from a normally distributed population. As measures of normalcy, skewness and kurtosis were used throughout this research project. A distribution's symmetry or lack of symmetry may be measured using the skewness statistic. It examines the degree to which the data have deviated from a normal distribution and determines whether or not the data have a normally distributed distribution. A severely skewed distribution is characterized by skewness values that are either less than -1 or larger than 1. A moderate degree of skewness is defined as a skewness value between -1 and -0.5 or 0.5 and 1, respectively. When the skewness value is between -0.5 and 0.5, the distribution is said to be fairly symmetric. When compared to a normal distribution, the peakedness or flatness of a distribution is evaluated using the kurtosis statistic. A kurtosis rating of +/-1 indicates that the data is almost exactly distributed according to a normal curve. When compared to a normal distribution, a distribution is considered to have a peak if its kurtosis value is larger than or equal to -1, while negative kurtosis values that are more than or equal to 1 suggest that the tail of the distribution is more truncated than that of a normal distribution.

The degree of correlation between three or more independent variables may be analyzed using multi-collinearity tests. A statistical technique called the VIF may be used to the model to determine how strongly one independent variable is related to another. Values of the VIF that are less than four are deemed to be acceptable and suggest a moderate to nearly nonexistent correlation among the variables. On the other hand, values that are larger than four indicate a significant correlation among the variables. The presence of homoscedasticity shows that the connection being analyzed holds true for all ranges of the target variable. This suggests that the differences between the values that are being explored are limited and comparable in nature.

4.3.1 Normality Test

A normality test was performed to see whether the data were distributed normally. As measures of normalcy, skewness and kurtosis were analyzed in this research. The findings of the examination are detailed in table 4.4 below.

Table 4.4: Normality test

Cronbach's Alpha	N of Items
.883	6

Source: Research Findings (2023)

Cronbach's alpha is a measure of internal consistency (for additional detail, see table 4.4) that reveals how cohesively a set of objects fits together. It's used as a yardstick to evaluate the accuracy of the scale. Just because the alpha parameter has a "high" value does not mean the measure is necessarily dimensional. If it is additionally required to establish that the scale in question consists of just one dimension, then further investigations may be carried out in addition to evaluating the scale's internal consistency. Exploratory factor analysis is one method that may be used to look at dimensions. In contrast to other statistical tests, Cronbach's alpha is a coefficient of dependability (or consistency), which is just another word for "consistency." The alpha score of.883 for these six items suggests a high degree of internal consistency.

The skewness value for fraud was found to be -0.656, and the kurtosis value was found to be -0.849, as shown in table 4.5. Both of the numbers were found to be within the usual range, which indicates that the distribution was normal. A statistical measure called skewness is used to evaluate the degree to which a probability distribution is asymmetrical. It provides a numerical representation of the degree to which the data are biased or skewed to a certain direction. Distributions with a positive skewness have longer right-hand tails, whereas those with a negative skewness have longer left-hand tails. When looking for patterns and outliers in a dataset, skewness is a helpful metric to utilize. A model's assumptions may be broken or the feature's significance may be downgraded if its values are skewed if it is used as an independent variable (feature).

Positivity skews the right-tailed distribution, whereas negativity skews the left-tailed one. One may say that this is the antithesis of a positively skewed distribution. An example of

a negatively skewed distribution model is one in which the bulk of the data is on the right-hand side of the graph while the tail of the distribution extends out to the left. If the data is negatively skewed (much of the information is shifted to the left), then the median will be higher than the mean. If the central tendencies of a distribution are all negative, rather than positive or zero, we say that it has a negative skew. The term "negatively skewed distribution" describes this shape of distribution. Each step in the process from identifying risks to assessing them to measuring them to monitoring them to reducing them had a skewness number that was negative and skewed to the left: -0.718, -1.240, -0.729, -1.065, and -0.817.

When the kurtosis value is positive, it means that the tails are longer and the distribution is more peaked, but when the value is negative, it says that the tails are shorter and the distribution is flatter. The kurtosis statistic is useful for examining the properties of a dataset, including its outliers. The degree to which a distribution has tails is referred to as its kurtosis, and it may be measured. The term "tailedness" refers to the frequency with which outliers appear. The term "peakedness" refers to the degree to which the values of a data distribution are concentrated in close proximity to the mean. Data sets that have a high kurtosis often exhibit a noticeable peak around the mean, drop quickly, and have large tails in their distributions. Data sets that have a low kurtosis are less likely to have a high peak and more likely to have a flat top around the mean. The kurtosis for skewness value for operational risk identification was -0.605, while the operational risk measurement had a value of -0.725. Both of these values were negative. Despite having a

positive kurtosis, operational risk assessment, operational risk monitoring, and operational risk mitigation all had respective values of 0.844, 0.241, and 0.226 respectively.

Table 4.5: Skweness and Kurtosis Statistics

Descriptive Statistics

	N	Mean	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
FRA	39	4.2410	-.656	.378	-.849	.741
IDE	39	4.7603	-.718	.378	-.605	.741
ASE	39	4.8590	-1.240	.378	.844	.741
MEA	39	4.5769	-.729	.378	-.725	.741
MON	39	4.4821	-1.065	.378	.241	.741
MIT	39	4.7969	-.817	.378	.226	.741
Valid N (listwise)	39					

Source: Research Findings (2023)

4.3.2 Multi-Collinearity

To measure the degree of correlation between the free variables, multi-collinearity tests were carried out. Multi-collinearity was analyzed with the use of the variance inflation factor (VIF).

Table 4.6: Collinearity Statistics

	Tolerance	VIF
Operational Risk Identification	.067	15.014
Operational Risk Assessment	.219	4.561
Operational Risk Measurement	.084	11.973
Operational Risk Monitoring	.153	6.555
Operational Risk Mitigation	.677	1.478

Source: (Secondary Data, 2022)

Table 4.6 above revealed that the VIF values for operational risk identification, operational risk assessment, operational risk measurement, operational risk monitoring and operational risk mitigation were 15.014, 4.561, 11.973, 6.555 and 1.478 respectively. This was an indication that the variables were not correlated to any other factor in the study. The residuals are approximately normally distributed. The concept of multicollinearity investigates the degree to which the variables are intercorrelated with one another. In the research, multicollinearity was analyzed with the use of the variance inflation factor. If VIF is equal to 1, then there is no connection; if it is between 1 and 5, then there is a moderate correlation; and if it is more than 5, then there is a strong correlation.

4.3.3 Homoscedasticity

Homoscedasticity was tested via histogram. The test results were presented graphically on a histogram.

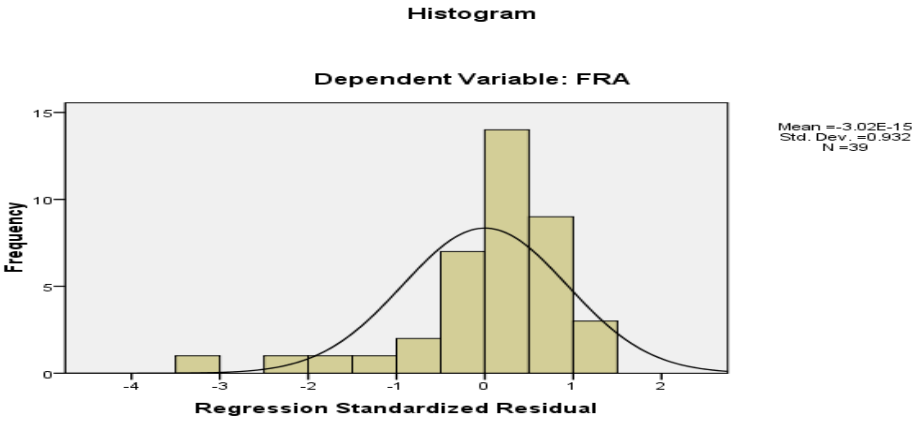


Figure 4.5: Homoscedasticity

Source: Research Findings (2023)

From figure 4.5 it was evident that a relationship did exist between the regression standardized residual and frequency of the dependent variable loan performance. Thus homoscedasticity assumption was not violated by the data set.

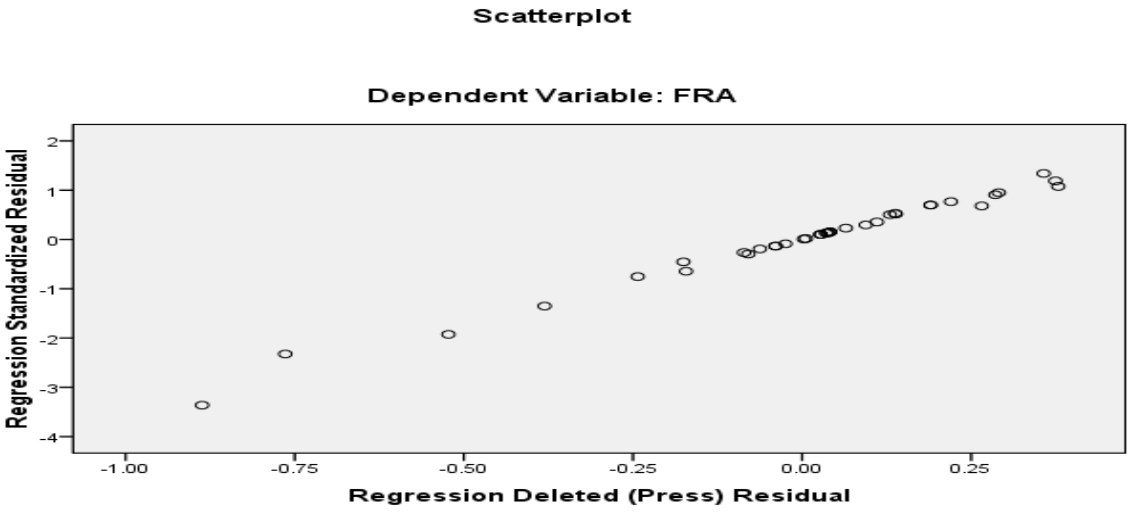


Figure 4.6 Normal P-P Plots

Source: Research Findings (2023)

It was evident from the normal p-p plot that the data obtained from the research were grouped close to the normal line of best fit, and there were no notable deviations or outliers in the data. As a result, it was established that the data used for the investigation originated from a normal distribution.

Table 4.7: Autocorrelation

Autocorrelation	
Durbin-Watson Statistic	2.153

Source: Research Findings (2023)

The Durbin-Watson test is helpful for determining whether or not a statistical model's or regression analyses' residuals exhibit autocorrelation. The Durbin-Watson test statistic is guaranteed to fall between zero and four, inclusive, at all times. When set to 2.0, it indicates that the sample exhibits no autocorrelation. Autocorrelation levels between 0 and less than 2 are considered positive, whereas autocorrelation values between 2 and 4 are considered negative. The Durbin-Watson Statistic was found to be 2.153 when it was looked up in the autocorrelation table. This number is close to 2, roughly. Therefore, it was understood to imply that there was no autocorrelation present in the variables that were subject to the inquiry.

Table 4.8: Levene's Test

	Levene Statistic	df1	df2	Sig.
Based on Mean	0.664	39	5	0.591
Based on Median	0.525	39	5	0.485
Based on Median and with adjusted df	0.892	39	5	0.816
Based on trimmed mean	0.985	39	5	0.214

Source: Secondary Data, (2022)

A significant level of 0.591 was found using Levene's test, which was based on the mean. This threshold of significance was higher than 0.05, which is the standard deviation. This indicates if the p-value for the Levene test is greater than 0. 05, then the variances are not significantly different from each other (i.e., the homogeneity assumption of the variance is met). If the p-value for the Levene's test is less than .05, then there is a significant difference between the variances.

4.4 Descriptive Statistics

Descriptive statistics enable a researcher to organize, simplify and quantify basic characteristics of a data set. Summaries derived from descriptive statistics provide more information for the variables under study as well as help highlight potential relationship among the variables. The research looked at a variety of descriptive statistics, including the lowest, maximum, mean, and standard deviation. The minimum highlights the lowest point in the data collection, whereas the maximum emphasizes the greatest point, bringing attention to both extremes. The mean shows how far off each data point is from the group

average; whereas the standard deviation shows how far apart individual data points are from the mean. Standard deviations that are larger than the mean indicate that the majority of the points in the data set are located a significant distance from the mean, while standard deviations that are less than the mean indicate that the most of the points in the data collection are clustered close to the mean. Table 4.9 presents the results of the investigation as they were found.

Table 4.9: Descriptive Statistics

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Bank Fraud	39	3.40	4.80	4.2410	.38369
Operational Risk Identification	39	4.26	5.00	4.7603	.24355
Operational Risk Assessment	39	4.30	5.00	4.8590	.21364
Operational Risk Measurement	39	4.00	4.90	4.5769	.28605
Operational Risk Monitoring	39	3.90	4.80	4.4821	.24156
Operational Risk Mitigation	39	4.40	5.00	4.7969	.15154
Valid N (listwise)	39				

Source: Research Findings (2023)

From the descriptive statistics table, it was established that Bank Fraud had a minimum value of 3.40 and a maximum of 4.80. The mean of Bank Fraud was established at 4.2410 with a S.D of 0.38369. The Operational Risk Identification had a minimum of 4.26 and a

maximum of 5.00. The mean of the Operational Risk Identification was established at 4.7603 with a S.D of 0.24355. The Operational Risk Assessment had a minimum of 4.30 and a maximum of 5.00. The mean of the Operational Risk Assessment was established at 4.8590 with a S.D of 0.21364. Operational Risk Measurement had a minimum of -4.00 and a maximum of 4.90. The mean of the Operational Risk Measurement was established at 4.5769 with a S.D of 0.24156. Operational Risk Monitoring had a minimum of 3.90 and a maximum of 4.80. The mean of the Operational Risk Monitoring was established at 4.4821 with a S.D of 0.24156. Operational Risk Mitigation had a minimum of 4.40 and a maximum of 5.00. The mean of the Operational Risk Mitigation was established at 4.7969 with a S.D of 0.15154.

4.4.1 Operational Risk Identification Descriptive Statistics

On the assessment of the satisfaction levels of operational risk identification the descriptive results on Table 4.10 indicate a narrow dispersion that is generally very high.

Table 4.10 Means and Standard Deviations of Operational Risk Identification

Description	Mean	SD
The bank conducts a comprehensive and methodical analysis of risks	4.5128	1.5824
Alterations to the risks are recognized and acknowledged in accordance with the tasks and responsibilities of the bank.	4.5385	1.6490
The bank is familiar with the pros and cons of risk management approaches used by other financial organizations.	4.3077	1.3393
The bank has devised and put into practice methods for the methodical spotting of opportunities.	4.6410	1.7146
It is of the utmost importance for the bank to use the most cutting-edge methods for risk detection.	4.5641	1.6471

Source: Research Findings (2023)

On the assessment of the satisfaction levels of operational risk identification the descriptive results on Table 4.10 indicate a narrow dispersion that is generally very high. This shows that the banks conducts a comprehensive and methodological analysis of risk (mean=4.5128, SD =1.5824), pros and cons of risk management (mean=4.3077, SD =1.3393) and the banks are cutting-edge methods for risk detection (mean=4.6410, SD =1.7146). The scores are closely distributed. Based on this, operational risk identification is highly embraced in the banks.

4.4.2. Operational Risk Assessment Descriptive Statistics

The scores on operational risk assessment are closely distributed are all as shown in table 4.11.

Table 4.11: Means and Standard Deviations of Operational Risk Assessment

Description	Mean	SD
The bank investigates and assesses the many possibilities it has available to fulfill its goals.	4.1795	1.2789
The reaction of the bank to the risks that were examined comprises prioritizing the risks and choosing those that need active management.	4.1795	1.2339
The bank conducts a review to determine whether or not the customer is creditworthy.	3.7949	1.1021
Before extending financial assistance the bank conducts a thorough examination.	3.3077	1.0816
The bank uses a computerized auxiliary system to forecast potential gains and risk management shifts.	4.3846	1.1349

Source: Research Findings (2023)

The bank investigates and assesses the many possibilities it has available to fulfill its goals (Mean=4.1795, SD =1.2789), extending financial assistance in the form of capital or credit, the bank conducts a thorough examination that takes into account the applicant's history, ability, circumstances, and collateral had the lowest mean scores (mean=3.3077, SD =1.0816) and the use computerized auxiliary system to forecast potential gains and risk management shifts had the highest mean (mean=4.3846, SD =1.1349).

4.4.3. Operational Risk Measurement Descriptive Statistics

From table 4.12 banks generates monthly report of operational risk on a regular basis had the highest mean of 4.9487 and the highest S.D of 2.1003. The use of quantitative analytic methods had the lowest mean of 4.7692 and a S.D of 1.6655.

Table 4.12: Means and Standard Deviations of Operational Risk Measurement

Description	Mean	SD
An evaluation of the risks faced by the bank is carried out with the use of several quantitative analytic methods.	4.7692	1.6655
Methods of qualitative analysis are used to conduct risk assessments on this financial institution (e.g. high, moderate, low)	4.8205	1.7818
This financial institution evaluates the possibilities that dangers may materialize.	4.8718	1.9678
The bank makes decisions based on a combination of quantitative data and human judgment.	4.8974	2.0343
The bank generates a monthly report of operational risk on a regular basis.	4.9487	2.1003

Source: Research Findings (2023)

4.4.4. Operational Risk Monitoring Descriptive Statistics

From the above table 4.13 monitoring the efficiency had the highest mean of 4.7179 and the highest S.D of 1.7730. The unified mechanism for reporting risk across all levels of management had the lowest mean of 4.4103 and a S.D of 1.3994.

Table 4.13: Means and Standard Deviations of Operational Risk Monitoring

Description	Mean	SD
Monitoring the efficiency with which risk management is being carried out is an essential component of regular management reporting.	4.7179	1.7730
The bank maintains a degree of control that is commensurate with the dangers that it is exposed to.	4.5641	1.5861
The bank has created a unified mechanism for reporting risk across all levels of management.	4.4103	1.3994
Activities carried out inside the bank, such as reporting and communicating with one another, contribute to the efficient management of risk.	4.5385	1.7899
The evaluation of the effectiveness of the various controls and risk management procedures already in place is part of the bank's response to risk.	4.6923	1.7733

Source: Research Findings (2023)

4.4.5 Operational Risk Mitigation Descriptive Statistics

Table 4.14 indicates that the company trains insured parties on ways to avoid or minimize the chances of losses occurring, got the highest mean score of 4.8718 and the greatest SD score of 1.9050, according to the table that was just shown. With a mean of 4.7692 and a SD of 1.6655, the assignment of clear obligations by the banks to oversee risk reduction earned the lowest score possible. Having a mechanism to transfer certain risks to third parties, such as through reinsurance (mean=4.7436, SD =1.8421), group prepared to assist

prevent disaster-related harm and keep operations running (mean=4.8462, SD =1.8426), and a response to security breaches and cybercrime attacks (mean=4.7949, SD =1.9043).

Table 4.14: Means and Standard Deviations of Operational Risk Monitoring

Description	Mean	SD
The bank have a disaster mitigation organization in place to mitigate damage and help continue business in the event of disaster	4.8462	1.8426
A Manager has been assigned with clear responsibility to monitor risk mitigation.	4.7179	1.6493
The company has a mechanism to transfer certain risks to third parties eg. Through reinsurance	4.7436	1.8421
The company trains insured parties on ways to avoid or minimize the chances of losses occurring	4.8718	1.9050
Propose a response to security breaches and cybercrime attacks	4.7949	1.9043

Source: Research Findings (2023)

4.4.6. Computer Fraud Descriptive Statistics

According to the table 4.15 the mean score for computer fraud was 4.2336. The practice of regularly changing passwords and not enabling computers or web browsers to keep login names or passwords received the highest mean score of 4.5385. It had a SD of 1.1249. The most significant factor in the decrease of computer fraud was good training for both customers and workers, which resulted in the lowest mean of 3.9744 and the smallest SD of 1.1713. The following is a list of the means and standard deviations for additional indicators of computer fraud: There are fraud reporting centers and hotlines (mean=4.2821, SD=1.2727), there is shuffling and obligatory vacations for staff (mean=4.3333, SD=1.2720), and there is use of ICT protection tools such as passwords and firewalls (mean=4.1795,SD=1.4004) There is an establishment of computer fraud

policy (mean=4.0256, SD =1.3256), there are fraud reporting centers and hotlines (mean=4.2821, SD=1.2727), Use of analytical tools to detect and prevent fraud(mean=4.3077, SD=1.2093) ,Staff are trained to detect and prevent fraud (mean=4.0256, SD=1.3630), Antivirus, anti-spyware, malware, adware protection and current software are installation (mean=4.4359, SD=1.4780).

Table 4.15: Means and Standard Deviations of Computer Fraud

Description	**Mean**	**SD**
Computer fraud policy is establishment	4.0256	1.3256
There are fraud reporting centers and hotlines	4.2821	1.2728
There will be personnel reorganization as well as required vacation time.	4.3333	1.2720
Use of information and communications technology (ICT) protection mechanisms such as passwords and firewalls.	4.1795	1.4004
The detection and prevention of fraud via the use of analytical technologies.	4.3077	1.2093
Training that is both helpful to staff and helpful to consumers may lead to a decrease in computer fraud.	3.9744	1.1713
The staff has received training to recognize and prevent fraudulent activity.	4.0256	1.3630
The most recent versions of antivirus software, anti-spyware software, malware protection software, and adware protection software are installed.	4.4359	1.4780
Altering passwords on a regular basis	4.5385	1.1249
	4.2336	

Source: Research Findings (2023)

4.4.7 Payment Fraud Descriptive Statistics

According to the data shown in table 4.16, the mean value for payment fraud was 3.8718. It is worth noting that the highest mean value of 4.4872 was observed for a centralized fraud-related information database pertaining to a certain payment type. It had a S.D of 1.4112. Establishing fraud reporting centers and hotlines had the lowest means of 3.4103and a S.D of 1.3451. The means and S.D for other indictors of computer fraud are as follows: All payment instruments with huge amounts should be referred to the issuing bank before payment (mean=3.6154, SD =1.1983, There is a detailed policy and procedure in place regarding online payments and EFT activities (mean=3.4872, SD=1.1249), Monitoring bank accounts on a regular basis for any unusual or illegal behavior and promptly reporting any suspicious activity (mean=3.5897, SD=1.0466), When doing financial transactions, using a wired network rather than a wireless one whenever it is feasible (mean=3.9231,SD=1.2306) and there is human review of payment transactions (mean=4.1282, SD=1.3002).

Table 4.16: Means and Standard Deviations of Payment Fraud

Description	**Mean**	**SD**
Staff members are provided with the necessary logistics and infrastructure to enable them perform their duties diligently	4.3333	1.2492
All payment instruments with huge amounts should be referred to the issuing bank before payment.	3.6154	1.1983
Establishing fraud reporting centers and hotlines	3.4103	1.3451
There is a detailed policy and procedure in place regarding online payments and EFT activities.	3.4872	1.1249
Monitoring bank accounts on a regular basis for any kind of illegal or suspicious behavior and promptly reporting any kind of suspicious conduct	3.5897	1.0466

that is discovered		
When doing financial transactions, using a wired network rather than a wireless one whenever it is feasible.	3.9231	1.2306
The processing of financial transactions is subject to audit by humans.	4.1282	1.3002
For one sort of payment, there is a centralized database that stores information linked to fraud.	4.4872	1.4112
	3.8718	

Source: Research Findings (2023)

4.4.8 Credit Card Fraud Descriptive Statistics

From table 4.17 credit card fraud had a mean of 3.69238 with the highest mean being 4.5641 i.e. use of AVS as a security technique used to prevent the online credit card fraud. It had a S.D of 1.5954. Sending card and PIN separately had the lowest means of 2.9744 and a S.D of 1.1151.

Description	Mean	SD
We have seen a relatively modest number of instances of card counterfeiting fraud.	4.3846	1.6677
We use a security measure known as Address Verification Service (AVS), which helps prevent fraudulent usage of credit cards over the internet.	4.5641	1.5954
We determine whether or not repeat consumers should be included to our Positive or Negative List by comparing their purchase histories to those of other customers.	4.1026	1.5639
Customer Authentication is a method that is used to verify that consumers who want to make a purchase are in fact allowed to do so.	3.6410	1.3236
Card Verification Value (CVV) is a security feature that is used to prevent fraud	3.6667	1.2641
Make that the customer's state ID card is legitimate by checking the machine-readable magnetic stripe or 2-D bar code on their driver's license or another form of state-issued identity.	2.9744	1.1151

Authentication may be accomplished by the use of biometrics, such as fingerprints, hand geometry, retinal patterns, speech patterns, and other similar characteristics.	3.2308	1.1552
During the account application process or at the point of sale, there is decision assistance available in real time	3.5641	1.2044
We have seen a relatively modest number of instances of card counterfeiting fraud.	3.1026	1.0984
	3.6923	

Source: Research Findings (2023)

4.5 Correlation Analysis

The goal of a correlation analysis is to measure the degree of linearity between two variables. The strength of a linear connection may be quantified using the correlation coefficient, often known as r, which is used to assess correlation. When the value of r is between 0 and 0.5, it indicates that the two variables have a moderately positive association. If the value of r is between 0.5 and 1, a significant positive association exists between the two variables. When r is between 0 and -0.5, a mild negative association exists between the two variables. When the value of r is between -0.5 and 1, a significant negative association exists between the two variables. The correlation table includes the findings from the study's investigation of the correlation between variables.

Table 4.18 Correlations Analysis

		IDE	ASE	MEA	MON	MIT	FRA
IDE	Pearson Correlation	1					
	Sig. (2-tailed)						
	N	39					
ASE	Pearson Correlation	-.293	1				
	Sig. (2-tailed)	.000					
	N	39	39				
MEA	Pearson Correlation	.938**	-.403	1			
	Sig. (2-tailed)	.000	.000				
	N	39	39	39			
MON	Pearson Correlation	.877**	-.311	.896**	1		
	Sig. (2-tailed)	.000	.000	.000			
	N	39	39	39	39	39	
MIT	Pearson Correlation	.223	.416	.280	.394*	1	
	Sig. (2-tailed)	.173	.023	.004	.013		
	N	39	39	39	39	39	39
FRA	Pearson Correlation	-.504**	-.363*	-.647**	-.644**	-.339*	1
	Sig. (2-tailed)	.001	.023	.000	.000	.035	
	N	39	39	39	39	39	39

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

From table 4.18 there is an indication that the correlation between the bank fraud when compared ORMP as measured by the five variables of operational risk although the correlations were weak negative correlations: The correlations between these processes are as follows: identifying operational risks (r=-0.504), assessing operational risks (r=-0.363), measuring operational risks (r=-0.647), monitoring operational risks (r=-0.644), and mitigating operational risks (r=-0.339). The results also show a moderately positive correlation between operational risk mitigation and operational risk identification

(r=0.223), operational risk assessment (r=0.416), operational risk measurement (r=0.280), and operational risk monitoring (r=0.394). The results also show a favorable association between identifying operational risks and taking steps to reduce them. Monitoring, identifying, and quantifying operational risks are all intertwined in a way that is both substantial and good. There is a 0.877 connection between finding operational risk and a 0.896 correlation between assessing operational risk. That is to say, if one goes up, the other one will go up as well. There is also a modest negative link between operational risk monitoring and operational risk assessment, with a negative correlation of -0.311. There is also a substantial positive link between measuring operational risk and identifying operational risk (r=0.938), which indicates this relationship is rather robust. The correlation between measuring operational risk and assessing operational risk is -0.938, which indicates a negative link between the two. In conclusion, there is a link between identifying operational risks and assessing operational risks that is characterized by a negative correlation (r = -0.293). Additionally, the correlational link between the independent variables and the dependent had a p value that was less than.005.

4.6 Regression Analysis

Finding out whether the connection between the dependent and independent variables is linear is the primary purpose of a regression study. It may also be used to measure how much of an effect each independent variable has on the variable under study (the dependent variable). The researchers used a regression analysis to look at the effects of interest rate changes on loan profitability. The model summary, ANOVA table, and Coefficients table all provide concise summaries of the study's findings.

The model summary also determines the proportion of the dependent variable's variance that can be explained by the model. The ANOVA tables reveal whether the model is appropriate for predicting the dependent variable, while the coefficients table reveals the relative importance of each independent variable to the accuracy of the prediction. Results were based on an analysis of data collected especially for the study, which are shown.

4.6.1 Model Summary

This section displays the primary tables that were used in order to get an understanding of linear regression. These tables were prepared using SPSS. The Model Summary may be found in Table 4.18, which can be seen below:

Table 4.19: Model Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.770[a]	.593	.531	.26280

a. Predictors: (Constant), MIT, ASE, IDE, MON, MEA

The values for R and R^2 are shown in the Model Summary. The value of R, which indicates the strength of a connection, is 0.881 in this particular instance. The R number may vary from minus one to plus one, and the direction of the connection is indicated by the sign, which can be positive or negative. A high degree of correlation was found, suggesting a strong positive relationship in the investigation. If the R value is high, the model is a good match for the data. The R Squared column, often known as the R^2 value, displays the percentage of the total variation in the dependent variable that can be accounted for by the independent variables. An R^2 value of 59.3 percent is shown in

Table 4.18, indicating that the linear model adequately explains the data for the dependent variable. In addition to explaining which model provides the most faithful picture of reality, the adjusted R^2 also plays a crucial part in selecting the optimal model. The adjusted R^2 value in this case is 59.3 percent. The model report made it very clear that R Square was 0.593. As calculated by computer fraud, payment fraud, and credit card fraud, operational risk assessment, operational risk identification, operational risk measurement, operational risk monitoring, and operational risk mitigation accounted for 59.3% of the variation in bank fraud. While other factors not included in the model accounted for 40.7% of the variance.

4.6.2 Analysis of Variance

The coefficients table is the third table that can be derived from SPSS with the use of regression analysis. By glancing at the "Sig." column in the coefficients table, one may evaluate whether or not the independent variables provide a statistically significant contribution to the model that is being applied. The direction of the correlations may be determined from the coefficients table. Beta coefficients that were not standardized were used in order to assess the influence that each of the independent variables had on bank fraud.

Table 4.20: ANOVA Analysis

ANOVA[b]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	3.315	5	.663	9.600	.000[a]
	Residual	2.279	33	.069		
	Total	5.594	38			

a. Predictors: (Constant), MIT, ASE, IDE, MON, MEA

b. Dependent Variable: FRA

Predictions for the outcome variable from the regression model are statistically significant if the p value from the Anova Table is less than 0.05. Table 4.19 shows that the regression model is a very accurate predictor of bank fraud due to its statistical significance (F = 9,600; = 0.000). The results suggest that the model well describes the data. Results showed that the model was statistically significant for predicting bank fraud after controlling for operational risk assessment, operational risk identification, operational risk measurement, operational risk monitoring, and operational risk mitigation.

4.6.3 Coefficients

Findings from the regression coefficients table show that the model is fit to predict bank fraud operations risk assessment, operational risk identification, operational risk measurement, operational risk monitoring and operational risk mitigation is;

Bank Fraud = 0.430 -1.291Operational risk identification - 0.11Operations risk assessment - 1.223 Operational risk measurement + 0.784 Operational risk monitoring + 0.191 Operational risk monitoring

Table 4.21: Regression Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.430	1.577		.273	.000
	Risk Identification	-1.291	.554	-.820	-2.330	.026
	Risk Assessment	-.011	.007	-.200	-1.676	.003
	Risk Measurement	-1.223	.513	.912	2.383	.023
	Risk Monitoring	.783	.443	.493	1.770	.016
	Risk Mitigation	.191	.320	.075	.597	.050

a. Dependent Variable: Fraud

Source: Research Findings (2023)

According to the regression equation, if all operational risks were eliminated (zero for operational risk identification, zero for operational risk assessment, zero for operational risk measurement, zero for operational risk monitoring, and zero for operational risk mitigation), the resulting value for bank fraud would be 0.430. The beta coefficients of -1.291, -0.11, and -1.223 shows that the three processes of identifying, assessing, and measuring operational risk all had a negative effect on bank fraud. This means that for every 1 improvement in Operational risk identification, Operational risk assessment, and Operational risk measurement, the chance of bank fraud decreases by -1.291, -0.11, and -1.223 respectively.

4.7 Discussions of the Findings

According to the findings majority of banks take fraud as a big issue. Economic pressures inside the nation, new computer technology, more cunning criminals, inefficient legal systems, and shifting social norms are just a few of the reasons why bank fraud is expected to rise significantly in the medium and long term. The prevalence of fraudulent activities in the banking industry is likely to rise. The most prevalent forms of fraud were the theft of money, the forgery of checks, the unauthorized use of credit cards, and the use of stolen identities. Majority of fraud cases were computer fraud at 45% followed by credit card fraud at 30%. Payment fraud was 30% while other type of fraud was at 5%. Most of the in the banks were in the tune of Kshs 100million as indicated by the respondents, followed by frauds between 81million to 100million. The rates of fraud for the small amounts of less than 20 million were few.

Findings indicated that operations risk assessment, operational risk identification, operational risk measurement, operational risk monitoring, and operational risk mitigation accounted for roughly 59.3% of the variance in bank fraud. These results are derived from the OLS table introduced previously in this section. However, the model missed the mark for explaining 40.7% of the variation because of extra factors. An excellent fit of the regression line and confidence in the model's prediction ability are both shown by this robust coefficient determination. This finding also indicates that the data is well-fit to the line. The significance level at which the F value of 9.600 holds is 5%. This proves that there is a strong positive correlation between operational risk assessment, operational risk identification, operational risk measurement, operational risk monitoring, and operational

risk mitigation and bank fraud, which is consistent with the a priori expectation that these things should have such a relationship.

The findings of the studies presented earlier provide hints that the independent factors do, in fact, have a considerable influence on the fraudulent activity at the institutions. This suggests that the control measures made by the management of banks on ORM will be successful in the prevention of bank fraud to the extent that they are implemented. The results of Nyakarimi and Karwirwa (2015) are supported by this information, which shows that this is true. This indicates that banks may benefit from good strategies for ORM that can assist them in preventing computer fraud, payment fraud, and credit card fraud. Mohammad (2015) came to a similar conclusion, which is that there is a positive and statistically significant association between the two variables, which is consistent with the previous result. This suggests that enhancing compliance with ethical norms for banking might help prevent unethical activity in financial institutions like banks. These results are consistent with those obtained by Adeyanju (2014).

ORM has negative significant relationship with computer fraud, payment fraud and credit card fraud. The findings suggest that the incidence of bank fraud is inversely proportional to the level of operational risk that a bank faces. A plausible explanation for this finding is that customers of Kenyan banks have a high level of trust and loyalty towards their financial institutions, despite the fact that the banks face operational risks such as the failure of internal processes, people, or systems. Despite this, customers continue to support the banks by depositing money, lending money, and investing money in the banks.

CHAPTER FIVE: SUMMARY OF FINDINGS, DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

In this chapter, the discussion of the major data results, the conclusion reached from the highlighted findings, and the suggestion made in relation to those findings were provided. The findings and suggestions that were derived were centered on contributing to the achievement of the study's primary purpose.

5.2 Summary of Findings

The purpose of this research was to determine whether or not there was a correlation between the ORM procedures of Kenya's commercial banks and the incidence of bank fraud in the nation. The primary goal of this study is to analyze how successful ORM could affect commercial bank fraud in Kenya. Many hypotheses were formulated by the researcher and tested to see whether or not they were statistically significant in achieving the project's aims. The findings of the regression analysis showed which variables had a statistically significant impact and which did not have a meaningful impact on the outcome. According to the regression equation, the value for bank fraud would be 0.430 if all operational risk variables were set to zero. This includes operational risk identification, operational risk assessment, operational risk measurement, operational risk monitoring, and operational risk mitigation. Detection, evaluation, and quantification of operational risk all had negative beta coefficients, indicating that they all had an adverse effect on bank fraud. These unfavorable results were represented by the numbers -1.291, -0.11, and -1.223. This indicates that a drop in bank fraud of -1.291, -0.11, and 1.223 occurs for

every unit improvement in operational risk identification, operational risk assessment, and operational risk measurement.

In this case the adjusted R^2 = 59.3%. It was made very obvious that R Square was 0.593 from the model summary. This indicated that operational risk assessment, operational risk identification, operational risk measurement, operational risk monitoring, and operational risk mitigation were responsible for 59.3% of the variance in bank fraud as evaluated by computer fraud, payment fraud, and credit card fraud. However, 40.7% of the variance was caused by additional variables that were not taken into account by the model. The operational risk identification had a correlation of -0.504, the operational risk assessment had a correlation of -0.363, the operational risk measurement had a value of -0.647, the operational risk monitoring had a correlation of -0.644, and the operational risk mitigation had a correlation of -0.339. The results also show a moderately positive correlation between operational risk mitigation and operational risk identification (r=0.223), operational risk assessment (r=0.416), operational risk measurement (r=0.280), and operational risk monitoring (r=0.394). In addition, the results show that identifying operational risks and taking measures to reduce them are somewhat correlated with one another. Monitoring, identifying, and measuring operational risks have a strong beneficial relationship with one another. The identification of operational risk has a correlation of 0.877, and the measuring of operational risk has a correlation of 0.896. That is to say, if one goes up, the other one will go up as well. There is also a modest negative link between operational risk monitoring and operational risk assessment, with a negative correlation of -0.311. There is also a substantial positive link between measuring

operational risk and identifying operational risk (r=0.938), which indicates this relationship is rather robust. The correlation between measuring operational risk and assessing operational risk is -0.938, which indicates a negative link between the two. In conclusion, there is a link between identifying operational risks and assessing operational risks that is characterized by a negative correlation (r = -0.293). Additionally, the correlational link between the independent variables and the dependent had a p value that was less than.005.

5.3 Conclusion

First, it's important to understand that this study aims to assess how successful ORM affects bank fraud rates in Kenya's commercial banking sector. The researcher formulated three objectives to address the research question, and they were then merged with objectives that addressed the foundations of efficient operational risk management. The frequency of incidents involving operational risk has grown during the last two decades. The Basel Committee established the Principles of Sound ORM as a direct reaction to this movement. This investigation was necessary because there were knowledge gaps concerning operational risk. This study's findings indicated that operational risk had a modest and context-dependent effect on bank fraud. The three variables (classifications of operational risk) were significantly related to one another. Operational risk assessment, risk identification, risk measurement, risk monitoring, and risk mitigation in the context of computer fraud, payment fraud, and credit card fraud as surrogates for bank fraud. The findings of this study provide validity to the findings of Odi (2013), who studied how fraud affects the efficiency of commercial banks.

This research identifies identification, assessment, measurement, monitoring, and mitigation as the primary contributors to ORM methods. Other key contributors are monitoring and identification. Therefore, financial institutions are obligated by law to keep their computer systems patched and secure against hackers at all times. It was concluded that the most effective way of ORM was to monitor and adhere to the risk limits that were established.

Among specific common frauds identified were computer hacking, sending phishing emails and attempts to distribute malware. Altering of payment instructions and diversion of funds to a fraudulent account were also common in payment processes. Use of stolen credit cards and use of unauthorized credit card information to shop online was a major credit card fraud.

This research was conducted with the ultimate goal of improving financial institutions' ORM processes via the use of established, industry-wide best practices for ORM. If this were to occur, financial institutions would function more efficiently, resulting in less money being lost. Bank fraud may, according to the findings, be influenced by detection, evaluation, measurement, monitoring, and mitigation strategies. As a direct consequence of this, commercial banks are required to reduce their focus on the prevention of bank fraud while simultaneously upgrading their operating systems.

5.4 Recommendations

This report may be used by regulatory agencies like the CBK for the purpose of doing further analysis and making policy suggestions. All financial institutions may benefit from knowing how effective ORM strategies affect financial institution performance and fraud rates, which is what this research establishes. This research may be used by the financial institutions for the objectives of staff training and the enhancement of employee understanding about ORM methods. In addition, the Kenyan Banking Association (KBA) should establish strategic connections with the banking organizations of other countries. This would enable members to get access to specialized information and facilitate the development of network linkages that might be of use to the banking sector.

The qualitative assessments that were acquired were helpful in establishing the level of damage that was sustained and rating the risks. The risk portfolio may be portrayed in the form of a risk map or matrix, which details the organization's respective advantages, disadvantages, opportunities, and dangers. It was hypothesized from the responses that bank workers would have some prior exposure to ORM concepts and procedures. While most survey takers were confident that operational teams were provided with up-to-date procedures, some had skepticism. While the bank does conduct trainings on operational risk management, respondents felt that it was insufficient. The ORM group's declared mission is to identify hazards and take preventative measures against them.

For the purpose of making the Kenyan financial system more resistant to fraud, the Kenyan legal system needs to go through significant structural changes. In spite of the fact that banking fraud is not now seen as a serious problem, there is mounting evidence

to suggest that this will become an increasingly pressing issue in the coming years. As a way of delivering non-branch banking services, financial technology in the banking industry is gaining a lot of traction in Kenya and other countries, thus it is reasonable to anticipate that these statistics will continue to rise over time. This is one reason why these figures are projected to rise over time.

The results of the study are significant for all of the financial institutions in terms of having a better knowledge of the influence that effective ORM has on the performance of financial institutions. This research may be used by the financial institutions for the objectives of staff training and the enhancement of employee knowledge about operational risk management. In terms of the empirical contribution, the results of the study were distinct from those of the majority of the findings found in earlier studies. The reason for this is because secondary data in the form of financial statements for the banks were used in the research that was carried out. In addition, the primary focus of this investigation was on the many types of operational risk that are associated with bank fraud. Consequently, it contributed still another dimension to the analysis.

Based on the conversations with respondents, we can conclude that ORM helps banks succeed by reducing the frequency and impact of incidents within operational teams. There will be less of an effect on the company's bottom line and less risk to its reputation as a result of this. In addition, banks may suffer monetary and reputational losses due to operational risk. The possibility of a corporation making more money and gaining more positive public reputation improves when operational risk is minimized, and vice versa. Better financial results may be achieved via the management of operational risk. The

findings confirmed that Kenyan banks successfully manage operational risk, that bank employees are well-versed in the principles and methods of risk management used by their respective institutions that banks are enforcing techniques that allow them to cater for operational risk, and that operational risk improves bank results. Strong ORM procedures in Kenyan banks may account for these findings.

Among critical recommendations to enhance strong ORM procedures and minimize some of the common fraud cases picked were: Use of robust firewalls, 2 Factor authentication systems to protect and safeguard access to sensitive bank systems, 2 to 3 levels of authorization of payments with maker-checker process mandatory, call backs to customers before processing payments, secure and full proof process of delivering credit & debit cards to customers, having limits on the cards and a trigger mechanism to block cards when suspicious payments are detected.

5.5 Limitations of the Study

The study did not include other forms of financial institutions, such as microfinance or pension funds, since it was limited to CBK. This is a case-by-case problem, hence the findings can only be generalized to Kenyan community banks. To extrapolate these results to the whole financial sector, future research must include the many financial organizations that were omitted here. This research stands apart from the bulk of others on ORM methods and fraud since it used only primary data, as opposed to secondary data like bank financial statements.

Due to the fact that the researcher was interested in primary data, questionnaires were required to be prepared. Due to the fact that the respondents claimed that they were busy,

some of the surveys were never handed back in. The accessibility of the responses was another source of difficulty. As a direct consequence of this, the study was forced to transmit part of the surveys by email in order to reach all of the respondents who had been targeted.

The study's findings are grounded only in primary data; however, future research based on primary data will need to be bolstered by panel data culled from the financial accounts of numerous organizations.

5.6 Suggestions for Further Research

More work on the factors that affect electronic fraud at Kenya's other commercial banks is needed before the results of this study can be applied more broadly. Since the operations of other organizations, such as insurance and microfinance institutions, are distinct from those of banks, it is important to do research of this kind on these other types of businesses as well.

In further research, the scope of the topic may be expanded to include additional types of hazards, such as credit risk, market risk, and liquidity risk. This may be helpful in making comparisons and expanding one's knowledge of risk management in Kenya's banking industry. Research on the topic's qualitative aspects may also be carried out via the use of interviewing participants and holding focus groups in order to get an explanation of the topic's quantitative aspects. This will therefore lead to an improvement in the quality of the outcomes as a whole. In the future, other institutions, such as those who provide microfinance, may also be able to participate in the study.

REFERENCES

Adeyemi, A. (2010). Winning customers' confidence: The new banking focus. *The Guardian*, May 26: 25

Adeyemo A., K. (2012). Frauds in Nigerian Banks: Nature, Deep-Seated Causes, Aftermaths and Probable Remedies. *Mediterranean Journal of Social Sciences*, *3*(2), 279. Retrieved from https://www.richtmann.org/journal/index.php/mjss/article/view/11022

Agboola, A. A. (2001). Impact of Electronic Banking on Customer Services in Lagos, Nigeria. *Ife Journal of Economics and Finance*, 5(1 and 2)

Albrecht, W., Howe, K. & Romney, M. (1984). *Deterring fraud: The internal auditor's perspective.* The Institute of Internal Auditors Research Foundation. Altamonte Springs, FL

AlhawariS.,KaradshehL.,TaletA.N.,MansourE.,(2012).Knowledge- Based Risk Management framework for Information Technology project, *International Journal of Information Management (32),* 50– 65.

Appelbaum, S. & Shapiro, B. (2006). Diagnosis and Remedies for Deviant Workplace Behaviors. *Journal of American Academy of Business, Cambridge*; 14-15

Basel Committee on Banking Supervision. (2001) Consultative Document Operational Risk. *Bank of International Statements.*

Birindelli, G., & Ferretti, P. (2017). *Operational Risk Management in Banks*. London, UK: Palgrave Macmillan

Central Bank of Kenya http://www.centralbank.go.ke/ Accessed 2nd September, 2021.

Chandran, E. (2004). *Research methods: A quantitative approach with illustrations from Christian Ministries*. Nairobi: Daystar University.

Cheng T.C.E., Yip F.K., Yeung A.C.L., (2012). Supply risk management via guanxi in the Chinese business context: The buyer's perspective. *International Journal of Production Economics (139),* 3– 13

Coetzee, J. (2016). *Bank management in South Africa: A risk based perspective*. Cape Town: Juta & Co. [Google Scholar]

Cooper, D and Morgan, W. (2008). Case study research in accounting. *Accounting Horizons* 22 (2): 159-178.

Cressey, R.D. (1973). *Other people's money: A study in the social psychology of embezzlement.* Montclair, NJ Peterson smith.

Day, R. (2010). Applying the Fraud Triangle Model to the Global Credit Crisis. *Icelandic E-Journal of Nordic and Mediterranean Studies,* 5(1).

Dorminey, J, Fleming A, Kranacher, M and Riley, R. (2020). Beyond the Fraud Triangle. CPA Journal. http://viewer.zmags.com/publication/1fadbbed#/1fadbbed/20

Dorminey, J. (2012).The Evolution of Fraud Theory, *Issues in Accounting Education Journal*: Vol. 27, (2) (555-579).

Ekechi, J. (2019). Bank Frauds in Nigeria: Underlying causes, effects and possible remedies; *African Journal of Accounting, Economics, Finance and Banking Research Vol. 6.* No. 6.

Ernst & Young. (2012). *Top and Emerging Risks for Global Banking*. Retrieved from http://www.ey.com/Publication/vwLUAssets/Top_and_emerging_risks_for_global_banking/$FILE/Top_and_emerging_risks.pdf [Google Scholar]

Ferreira, S. (2015). *Measuring reputational risk in the South African banking sector (Dissertation- MA)*. North-West University.

Gillet, R., Hübner, G., & Plunus, S. (2010). Operational risk and reputation in the financial industry. *Journal of Banking & Finance*, 34(1), 224–235.

Huber, D. (2017). Forensic Accounting, Fraud Theory, and the End of the Fraud Triangle, *Journal of Theoretical Accounting Research*, (12(2), 28-48.

Jesper F. (2008). *occupational fraud –auditors' perceptions of red flags and internal control* Linkoping's University, Linkoping, Sweden

Kanu, S. I., & Okoroafor, E. O. (2013). The Nature, Extent and Economic Impact of Fraud on Bank Deposit in Nigeria. *Interdisciplinary Journal of Contemporary Research in Business*, Vol. 4 no. 9 pp. 253-264.

Kingsley, S., A. (2012). *Operational Risk and Financial Institutions: Getting Started.* Pp. 3–28.

Lokanan, M.E. (2014). How Senior Managers Perpetuate Accounting Fraud? Lessons for Fraud Examiners from an Instructional Case. *The Journal of Financial Crime,* 21(4): 411-423.

Lyambiko, M.R. (2015). The Effect of Operational Risk Management Practices on the Financial Performance in Commercial Banks in Tanzania. *Unpublished MBA Project, University of Nairobi.*

Matsueda, R, L. (2010). Differential Association Theory and Differential Social Organization." *Encyclopedia of Criminological Theory*, Sage Publications, 2010, pp. 899-907

Mohammad, A. (2010). Technology acceptance in Kenyan retail banking. *International Journal of Bank Marketing,* Vol. 6 No.4, :31-41.

Mohammad, I. (2015). The role of corporate governance in fraud reduction: A perception study in Saudi Arabia business environment. *Journal of Accounting and Finance, 15(2),* 119 –128.

Montgomery, D. (2013) *Introduction to Statistical Quality Control,* 7th ed. (Hoboken, NJ: John Wiley & Sons, Inc., 2013).

Mustaine, E. E., & Tewksbury, R. (2002). Workplace theft: An analysis of student-employee offenders and job attributes. *American Journal of Criminal Justice, 27* (1), 111-127.

Ngalyuka, C. (2013). The relationship between ICT utilization and fraud losses in commercial banks in Kenya. *International Journal of Business and Public Management, 2*(3), 56–59.

Nyakarimi, S. N. &., Karwirwa, M. (2015). Internal control system as means of fraud control in deposit taking financial institution in Imenti North Sub-Country. *Research Journal of Finance and Accounting*, 6(16), 118-128.

Nyakarimi, S. N. &.,Karwirwa, M. (2015). Internal control system as means of fraud control in deposit taking financial institution in Imenti North Sub-Country. *Research Journal of Finance and Accounting, 6(16),* 118-128.

Odi, N (2013). *Implications of Fraud on Commercial Banks Performance in Nigeria. Kogi State University*, Anyigba Kobi. Nigeria.

Ogechukwu, O. J. (2013). Bank Fraud and Its Effect on Bank Performance in Nigeria. *International Journal of Business and Management Invention*, 2(2).

Rajendran, M. (2012). Operational risks involved in banking industries. *Amity Global Business Review*, 7(1), 50–57.

Romānova, I. and Kudinska, M. (2020), "Banking and Fintech: A Challenge or Opportunity?", *Contemporary Issues in Finance: Current Challenges from Across*

Europe (*Contemporary Studies in Economic and Financial Analysis, Vol. 98*), Emerald Group Publishing Limited, Bingley, pp. 21-35.

Singleton, T, and Singleton, J. (2010). *Fraud Auditing and Forensic Accounting (4th Edition)*. New Jersey: Wiley & Sons; 2010.

Soltani, B. (2014). The Anatomy of Corporate Fraud: A Comparative Analysis of High Profile American and European Corporate Scandals. *Journal of Business Ethics*, DOI 10.1007/s10551-013-1660-z

Sutherland, E. (1947). *Principles of Criminology* (4th edition). Philadelphia: J. B. Lippincott Company.

Toroitich, A. (2018). Effect of Operation Risk Exposure On Financial Performance of Commercial Banks in Kenya. *Unpublished MSC Project*, University of Nairobi

Toroitich,A. (2018). Effect of Operation Risk Exposure On Financial Performance of Commercial Banks in Kenya. *Unpublished MSC Project*, University of Nairobi

Vardy, J. (2015). *Reputational Risk Management in Central Banks*. Canada: Bank of Canada.

Wells, J.T. (2005). *Principles of fraud examination*. London: John Wiley and Sons.

Wilhelm W. K. (2004). The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management. *Journal of Economic Crime Management*, 2(2), 8-10

APPENDICES

APPENDIX I: QUESTIONNAIRE

Please respond to the following questions by filling in the blanks that are given.

PART A: GENERAL INFORMATION

This section's goal is to collect some background data about your banking experience and you as an individual research participant.
Please tick [√] where appropriate or fill in the required information.

1. What is the Name of the Bank? _____

2. Where do you stand in the hierarchy of this organization? _____

3. How many years fall into each of your age brackets?

   (a) Below 30 years [ ]

   (b) Between 31-40 years [ ]

   (c) Between 41-50 years [ ]

   (d) Above 50 years [ ]

4. What is your gender?

   (a) Male [ ]

   (b) Female [ ]

5. Please mention the highest level of schooling you have completed.
   (a) Diploma [ ]
   (b) Undergraduate degree [ ]
   (c) Masters [ ]
   (d) PhD [ ]

6. How long have you worked for the bank's anti-fraud division in your present capacity?
   a) Below 3 years [ ]
   b) Between 3-5 years [ ]
   c) Between 6- 9 years [ ]
   d) Between over 10 years [ ]

PART B: OPERATIONAL RISK MANAGEMENT PRACTICES

□□ the second part of the survey is meant to collect data on different operational risk management techniques.

□□PLEASE TICK [√] WHERE APPROPRIATE OR FILL IN THE REQUIRED INFORMATION

To what extent are the following statements regarding ORMPon fraud in Commercial banks true

Please indicate 1=Not at all 2=little extent 3=Moderate extent 4=great extent 4=Very great extent

A	**Understanding Operational Risk Management:**	**1**	**2**	**3**	**4**	**5**
1	Across the board, the bank has an agreement on how to handle operational risk.					
2	In the bank, there is a good system in place for comprehending the several hazards that are there.					
3	The operational risk management responsibility has been outlined in detail and is understood by all employees within the bank.					
4	The bank as a whole has a crystal clear understanding of who is responsible for what with regard to operational risk management.					
5	The bank provides its customers with a comprehensive set of rules and recommendations to follow in order to effectively manage operational risk.					
B	**Operational Risk Identification**	**1**	**2**	**3**	**4**	**5**
6	The bank conducts a comprehensive and methodical analysis of the risks that are associated with each of the purposes and objectives that it has publicly stated.					
7	Alterations to the risks are recognized and acknowledged in accordance with the tasks and responsibilities of the bank.					
8	The bank is familiar with the pros and cons of risk management approaches used by other financial organizations.					
9	The bank has devised and put into practice methods for the methodical spotting of opportunities.					

10	It is of the utmost importance for the bank to use the most cutting-edge methods for risk detection.					
C	**Operational Risk Assessment**	**1**	**2**	**3**	**4**	**5**
11	The bank investigates and assesses the many possibilities it has available to fulfill its goals.					
12	The reaction of the bank to the risks that were examined comprises prioritizing the risks and choosing those that need active management.					
13	Before extending credit or carrying out transactions, the bank conducts a review to determine whether or not the customer is creditworthy.					
14	Before extending financial assistance in the form of capital or credit, the bank conducts a thorough examination that takes into account the applicant's history, ability, circumstances, and collateral.					
15	The bank uses a computerized auxiliary system to forecast potential gains and risk management shifts.					
D	**Operational Risk Measurement**	**1**	**2**	**3**	**4**	**5**
16	An evaluation of the risks faced by the bank is carried out with the use of several quantitative analytic methods.					
17	Methods of qualitative analysis are used to conduct risk assessments on this financial institution (e.g. high, moderate, low)					
18	This financial institution evaluates the possibilities that dangers may materialize.					
19	The bank makes decisions based on a combination of quantitative data and human judgment.					
20	The bank generates a monthly report of operational risk on a regular basis.					
F	**Operational Risk Monitoring**	**1**	**2**	**3**	**4**	**5**

21	Monitoring the efficiency with which risk management is being carried out is an essential component of regular management reporting.					
22	The bank maintains a degree of control that is commensurate with the dangers that it is exposed to.					
23	The bank has created a unified mechanism for reporting risk across all levels of management.					
24	Activities carried out inside the bank, such as reporting and communicating with one another, contribute to the efficient management of risk.					
25	The evaluation of the effectiveness of the various controls and risk management procedures already in place is part of the bank's response to risk.					
F	**Operational Risk Mitigation**	**1**	**2**	**3**	**4**	**5**
26	In the case of a natural catastrophe, the bank has a disaster mitigation organization in place to reduce the amount of damage and assist in the continuation of operations.					
27	Clear responsibility for monitoring risk mitigation has been delegated to a Manager who has been designated.					
28	The organization has a system in place to allow for the transfer of certain risks to other parties, for example. With the help of reinsurance					
29	The firm instructs insured parties on measures they may take to prevent or reduce the likelihood of suffering losses.					
30	Make a suggestion on how to react to the recent security breaches and acts of cybercrime.					

PART C: BANK FRAUD

Please tick [√] where appropriate or fill in the required information.

1. How would you characterize the extent of the fraud issue in the financial sector?

   Major problem [ ] Minor problem [ ] Not a problem [ ]

2. What type of fraud is predominant? (Circle any ***three*** at most)

   i. Computer Fraud

ii. Payment Fraud

iii. Credit Card Fraud

iv. Any Other Fraud (specify)_____

3. In a typical year, how much fraudulent activity do you estimate is uncovered by your bank? (Kshs Million)

   1-20 [ ] 21-40 [ ] 41-60 [ ] 61-80 [ ] 81-100[ ] Over 100[ ]

4. To what extent are the following statements regarding Bank Fraud in Commercial banks true Please indicate 1=Not at all 2=little extent 3=Moderate extent 4=great extent 4=Very great extent

A	**Computer Fraud**	**1**	**2**	**3**	**4**	**5**
1.	The development of a policy about computer fraud					
2.	There are locations for reporting fraud as well as hotlines.					
3.	There is personnel reorganization as well as mandated vacation time.					
4.	Utilization of information and communication technology security techniques such as passwords and firewalls					
5.	Utilization of analytic technologies in order to identify and stop fraudulent activity					
6.	Training that is both helpful to staff and beneficial to consumers may lead to a decrease in computer fraud.					
7.	The staff has received training to recognize and prevent fraudulent activity.					
8.	Virus protection, spyware protection, malware protection, adware protection, and up-to-date software are all installed.					
10	Changing passwords on a regular basis and preventing the computer or web browser from saving login names or passwords are also important security measures.					
B	**Payment Fraud**	**1**	**2**	**3**	**4**	**5**
11	Staff members are provided with the necessary logistics and infrastructure to enable them perform their duties diligently					
12	All payment instruments with huge amounts should be referred to the issuing bank before payment.					
13	Establishing fraud reporting centers and hotlines					
14	There is a detailed policy and procedure in place regarding online payments and EFT activities.					

15	Monitoring bank accounts on a regular basis for any kind of illegal or suspicious behavior and promptly reporting any kind of suspicious conduct that is discovered					
16	Whenever feasible, doing financial transactions through a wired network rather than a wireless network					
17	The processing of financial transactions is subject to audit by humans.					
18	For one sort of payment, there is a centralized database that stores information linked to fraud.					

C	**Credit Card Fraud**	**1**	**2**	**3**	**4**	**5**
19	We have experienced low counterfeit card fraud cases					
20	We make use of The Address Verification Service (AVS) is a security measure that is used to stop fraudulent usage of credit cards over the internet.					
21	We determine whether or not repeat consumers should be included to our Positive or Negative List by comparing their purchase histories to those of other customers.					
22	Customer Authentication is a method that is used to verify that consumers who want to make a purchase are in fact allowed to do so.					
23	Card Verification Value, often known as CVV, is a security feature that is intended to prevent fraud, particularly when the fraudster acquires the credit card data over the internet.					
24	Sending the card and PIN to the recipient at different times has helped alleviate difficulties of Frauds involving credit card use					
25	Make sure the customer's state ID is legitimate by checking the machine-readable magnetic stripe or two-dimensional bar code on their driver's license or another form of state-issued identification.					
26	Authentication may be accomplished by the use of biometrics, such as fingerprints, hand geometry, retinal patterns, speech patterns, and other similar characteristics.					
27	During the account application process or at the point of sale, there is decision assistance available in real time (for example, a score or warning on probable or known ID fraud or account takeover).					

THANK YOU

APPENDIX II: LIST OF COMMERCIAL BANKS IN KENYA

1	ABSA Bank Kenya
2	Access Bank Kenya
3	African Banking Corporation Limited
4	Bank of Africa Kenya Limited
5	Bank of Baroda (K) Limited
6	Bank of India
7	Citibank N.A Kenya
8	Consolidated Bank of Kenya Limited
9	Co-operative Bank of Kenya Limited
10	Credit Bank Limited
11	Development Bank of Kenya Limited
12	Diamond Trust Bank Kenya Limited
13	DIB Bank Kenya Limited

14	Eco bank Kenya Limited
15	Equity Bank Kenya Limited
16	Family Bank Limited
17	First Community Bank Limited
18	Guaranty Trust Bank (K) Ltd
19	Guardian Bank Limited
20	Gulf African Bank Limited
21	Habib Bank A.G Zurich
22	HF Group
23	I&M Bank Limited
24	Kingdom Bank Limited
25	KCB Bank Kenya Limited
26	Mayfair CIB Bank Limited
27	Middle East Bank (K) Limited
28	M-Oriental Bank Limited
29	National Bank of Kenya Limited
30	NCBA Bank Kenya PLC
31	Paramount Bank Limited
32	Prime Bank Limited
33	SBM Bank Kenya Limited
34	Sidian Bank Limited
35	Spire Bank Ltd
36	Stanbic Bank Kenya Limited

37	Standard Chartered Bank Kenya Limited
38	UBA Kenya Bank Limited
39	Victoria Commercial Bank Limited

Source: Bank Supervision Annual Report 2022