FRAUD IN THE BANKING INDUSTRY IN KENYA

A CASE OF COMMERCIAL BANK OF AFRICA, KENYA

BY

MARYANNE WAMUYU WANJOHI

UNITED STATES INTERNATIONAL UNIVERSITY AFRICA

SUMMER, 2014

FRAUD IN THE BANKING INDUSTRY IN KENYA

A CASE OF COMMERCIAL BANK OF AFRICA, KENYA

BY

MARYANNE WAMUYU WANJOHI

A Research Report Submitted to the Chandaria School of Business in Partial Fulfillment of the Requirement of the Masters in Business Administration (MBA)

UNITED STATES INTERNATIONAL UNIVERSITY AFRICA

SUMMER, 2014

COPYRIGHT

STUDENT'S DECLARATION

I, the undersigned, declare that this is research report is my original work and has not been submitted to any other college, institution or university other than the United States International University Africa in Nairobi for academic credit.

Signed:…… Date:……..

Maryanne Wamuyu (ID 636883)

This research report has been submitted for examination with my authority as the designated supervisor.

Signed:……..… Date:……..

Dr. Peter Kiriri

Signed:……..… Date:……..

Dean,Chandaria School of Business

DEDICATION

This research report is a special dedication to my family.

ACKNOWLEDGEMENT

I spare this page of the report to mention and acknowledge the special input of various pupils and institutions.

Firstly, I would like to acknowledge the mercies and grace of God which has seen me through the studies and in the conduct of this paper. It has been a hard journey but through the grace and mercy of God, it has finally come to fruition.

Secondly, I would like to thank my Supervisor Dr. Peter Kiriri who took his time to guide, advice and give his comments on the structure and content of the report. My supervisor was very helpful at all times and provided due advice and support when requested.

I would also like to thank my colleagues in the class and work place. They took time of their busy schedules to make notes and comments on the questionnaire at the pre-testing stage while my work colleagues provided data for this study. Their input was much appreciated and recognized.

To all those who contributed to the completion of this paper in one way or the other, I recognize and appreciate your efforts

Thank you all and God Bless You

ABSTRACT

This study sought to assess fraud in the banking industry in Kenya using Commercial Bank of Africa (CBA) as the case. The objectives of the study were: to establish the causes of fraud at CBA, examine the types of frauds committed and determine the appropriate strategies for prevention and control of fraud.

The study utilized a descriptive research design using CBA bank as the case. The study was conducted during the months of February and March 2014 using all employees of CBA with Nairobi County. A population of 68 employees representing 33% of the populations were included in the sample size using a stratified random sampling technique. Data for the study was collected using an online questionnaire for cost and convenience to all the respondents. However, the questionnaire was pretested for errors and relevance. Data collected was analyzed using SPSS vs. 20 for means, frequency distributions, standard deviations and modes. Analyzed data was presented using figures and tables for ease of interpretation and elaboration.

The study found that, fraud in CBA was accorded very high priority. The major causes of fraud in the bank were availability of opportunities for fraud, rationalization of fraud acts and pressure to commit fraud. Opportunities for fraud were present due to relaxed internal controls and accounting systems, inadequate supervision of subordinates, disregard for customer due diligence requirements and poor personnel policies.

Secondly, this study found that employee fraud was the most common fraud in the bank while third party fraud was second. Management fraud in CBA was very low. Some of the forms of fraud identified include: cash theft, use of forged documents, cards fraud, letters of credit fraud and impersonation.

Further, this study found that there were very effective strategies to prevent and control fraud. However, the most effective strategies for prevention and control of fraud are: use of ICT tools such as passwords and firewalls, strengthening of internal controls and systems, encouragement, communication, rewards and recognition of employees, performance management, improvement

and hiring systems and policies, use of expected and unexpected audits and use of analytical tools.

The study concluded that the most dominant factor influencing or accelerating fraud in CBA was the availability of opportunities for fraud. Further, the establishment of an ethical culture within the organization structure was critical in fraud management. Secondly, this study concluded that employees are the primary drivers of fraud through forging of documents, opening and management of fictitious accounts, claiming unearned benefits and computer frauds. On the other hand, management was the least contributors to fraud in the bank. The study further concluded that the most effective strategies for prevention and control of fraud were use of ICT tools, use of analytical tools, use of audits, strengthening of internal controls and application of customer and human resource management systems in the bank.

This study recommended that banks should implement systems and structures that reduce the opportunities for fraud. In addition to strengthening internal control systems and structures, banks can use ICT tools to reduce opportunities or instill punitive measures for employees engaging in fraud and fraud related incidences. Secondly, decentralize the functions of employees and ensure there are adequate authentication and control structures and systems in place to reduce employee fraud. Furthermore, employees should be regularly rotated between departments. This study recommends that ICT should form the core backbone for the prevention and control of fraud. This is because ICT can be used to track, identify and report cases of fraud.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACFE	Association of Certified Fraud Examiners
CBA	Commercial Bank of Africa
CBK	Central Bank of Kenya
CID	Criminal Investigation Department
CIMA	Chartered Institute of Management Accountants
PwC	PricewaterhouseCoopers
SPSS	Statistical Product for Social Sciences

CHAPTER ONE

1.0 INTRODUCTION

1.1 Background of the Problem

Risk is an inherent part of business life. Dynamic market relations increase the uncertainty of the environment where businesses and public organizations work. Risk management has become part of the organization activities and its main aim is to help all other management activities reach the organization's aims directly and efficiently. The changes in the environment require conditions attention for identification and control of risks (Tchankova, 2002).For a bank; risks are potential events that could influence the achievement of the organizations goals. Risk management therefore includes the conceit understanding of the events and how this events poses a threat. Fraud is one major risk that has potential significant negative impacts on the business. Fraud has an impact on the financial, brand image and reputation of the business (Chartered Institute of Management Accountants, 2009).

Fraud is an area of convergence for financial firms. Techsavy and young employees are leading the proliferation of insider fraud across most businesses in the work. This is opposed to insider fraud driven by supervisors, managers and superiors in the business. This has led to the ranking of fraud as one of the top five concerns for both banks and insurers in East Africa (PricewaterhouseCoopers [PwC], 2011). Institutional trust plays significant role in fraud detection and prevention. Modern business especially those operating online are using the principles of institutional trust, to improve and enhance effective governance as a strategy towards reducing fraud. Pan, Seow, Suwardy and Gay (2011) noted that ethics in business is one strategy that has a direct impact on fraud levels in the business.

A was survey done by PWC on 33 banks in Kenya, Tanzania, Zambia, Rwanda and Uganda participated in the late 2011 and 2010. In this study, the researchers sought to identify the risk identification and risk readiness levels in most local businesses. Over 50% of the

respondents to the study indicated that fraud as an area they needed to put more effort in preparedness (PwC, 2011). Furthermore, the economic survey of 2010 by PwC found that fraud incidents and cases had increased with higher margins in the year 2010 than in any other preceding year. Approximately, 90% of the respondents to the study indicated that most businesses in Kenya had recorded some cases of fraud while banks in the country had lost over Ksh 1.7 billion with just three months, August to October, 2010. This growth in the banking fraud was grounded on the rapid growth and expansion in banks which necessitated the implementation of complex multiple technological systems that promoted levels of fraud (PwC, 2011). Furthermore, the effectiveness of internal control systems in most banks is dwindling in comparison to the boldness and skills of highly networked and sophisticated fraudsters (PwC, 2011).

There was an upsurge in the prevalence of fraud in a review done in the third quarter on 2012. Categories of fraud included card frauds, insider, electronic and cheque frauds that were to be given keen focus (Central Bank of Kenya [CBK], 2012). CBK reviewed policy implications based on the trends and gave recommendations to Kenya Bankers Association. A total of 36 cases were reported of which 16 cases were successfully investigated and accused persons charged in court (Criminal Investigation Department [CID], 2013).

The study of fraud encompasses criminology, psychology, accounting, auditing, and management. According to Wels (1997), fraud growth and rise can be explained through a model that consist of three major factors: personal pressure, availability of opportunities and rationalization of the act/attitude. The Fraud model has its roots in the research noted by criminologist Donald Cressey. According to Cressey (1973), a sharable financial need is crucial to understanding behavior of one who violates trust to commit fraud. What is deemed non-sharable is in the eyes on the offender (Cressey, 1973).These ―non-sharable needs are divided into six basic types: violation of obligations, problems from personal failure, business reversals, physical violation, status gaining and employer-employee relationships (Cressey, 1973). Duress is caused by employee's perceived immediate need for assets (Cressey, 1973). Pressure causes the fraudster to undertake significant risks to obtain desired

resources. Opportunities for fraud occur when an employee acquires trust from an organization and abuses it or when the internal control systems in the organizations are very weak or absent (Cressey, 1973).

Justification of the acts of fraud as well as consistency of personal codes of ethics is one major cause of individual fraud (Hollinger and Clark, 1983). Other factors that lead to the increase and proliferation of fraud include: lack of experience and expertise in fraud detection, IT savvy employees, change resistance by superiors and older generations, lack of professionalism and competency in recruitment and selection of employees, poor and rigid judicial systems and procedures, small fines and court rulings that do not deter fraudsters and lack of effective communication and coordination of fraud tracking, detection and prevention by banks across the country (PwC, 2011). In addition to financial loss incurred by banks, the financial cost incurred arising out of court cases should encourage banks that to detect fraud in time to save money as well as damage to the banks credibility.

During the time of this research there were 44 banks operating in Kenya under the supervision of the regulatory body-Central Bank of Kenya. They can be categorized into groups based on three key factors namely: the capital base, core capital and branch network (PwC, 2009).

Commercial Bank of Africa (CBA) was the case for this study. Commercial Bank of Africa ltd was established in the year 1962 in the Tanzanian city of Dar es Salaam. The bank rapidly established branches in the East African region establishing branches in Mombasa, Nairobi and Uganda. Nevertheless, after the Tanzania's government's directive to nationalize all banks, CBA was reincorporated in the Kenyan capital in the year 1967 (CBA, 2012).

At the initial stages of incorporation and establishment, CBA operated as a wholly owned subsidiary of Societe Financiere pour les pays D'Outre Mer (SFOM) a Switzerland based conglomerate with interests in the Bank sectors such as Bank of America Commerzbank (whose interest was later sold to Dresdner Bank), Bank Bruxelles Lambert and Banque National de Paris (CBA, 2012

The Bank of America acquired all the shares of SFOM in the year 1980 leading the bank to become a subsidiary of Bank of America with local investors holding 16% of the shares. Commercial Bank of Africa underwent major reorganization and restructuring including the adaptation of the global payment systems utilized by the Bank of America to stimulate growth. However, the Bank of America later sold its stake to local investors though it remained as a management consultant for the bank through a management agreement before fully disposing its shares to the local investors. Currently, CBA has the accolade of being one of the biggest and innovative privately owned bank with branches in Kenya as well as Tanzania (CBA, 2012).

1.2 Statement of the Problem

In a study by Pan *et al.,* (2012), they concurred with other scholars on fraud that the use of the fraud triangle and other fraud frameworks are crucial in developing a conceptual model for the study and research on fraud. The financial markets have become innovative, creative as well as complex which has presented opportunities for fraud. According to Pan *et al.*, (2011), though the fraud triangle provide a framework for understanding fraud, not all types, causes and drivers of fraud are captured in the model. According to Pan *et al.*,(2011) trends, patterns and statistics such as personal characteristics have an impact on the levels of fraud though this is not captured in the model. Essentially, this requires additional investigation of the factors that drive fraud including personal characteristics. Furthermore, Pan recommended in their study that the study of fraud should seek to explore how personal traits and characteristics can be used to explain fraud and fraudsters. Furthermore, researchers ought to develop into a model how individual, firm and industry statistics motivate and drive fraud in organizations (Pan *et al.,* 2011).

While the research and recommendations by Pan *et al.* (2011), were undertaken in the European continent, very few studies have focused on fraud management and prevention in the African region and especially the East African region. Existing literature is concentrated in the West African region (Abdul and Tinusa 2012; Adenji, 2004; Adewumi, 2011)

especially in Nigeria with sparse studies in other regions in Africa. This has created a shortage in empirical evidence and studies on the local scene.

While fraud has been identified as a major challenge and issue in the Kenyan banking sector (CBK, 2013) very few scholars or studies have sought to establish the causes and strategies to combat fraud in the financial sector. This may have had a negative impact on policy making as policy solutions to fraud were not necessarily informed by empirical evidence. Nevertheless, the Central Bank of Kenya, the Capital Markets Authority and Kenya Bankers Association has various researchers who undertake private studies on behalf of the institutions especially on fraud management. However, these studies are not available to local citizens and researchers as they are institutional properties. This has created a research and practice gap in the region. This study sought to fill this gap by investigating the factors that contribute to fraud in the banking industry.

1.3 General Objectives

The general objective of this study was to assess fraud in the banking industry.

1.4 Specific Objectives

1.4.1 To establish factors contributing to fraud in the banking industry

1.4.2 To examine the types of frauds committed against banks

1.4.3 To determine appropriate strategies of preventing and controlling fraud

1.4 Importance of the Study

The research is of use to decision makers in the banking industry, policy makers, scholars and the researchers.

1.5.1 Commercial Bank of Africa Ltd

Auditor's security teams, hiring managers and operations managers can have a better understanding of the factors that contribute to fraud. CBA can draw from the findings of this study on the different ways of mitigating fraud.

1.5.2 Banking Industry

Banks are able to gain a deeper understanding of fraud and adopt appropriate strategies to mitigate loss resulting from fraudulent activities. This is due to new knowledge and information available as a result of the study.

1.5.3 Policy Makers

This may include Kenya Bankers Association, Central Bank of Kenya and Banking Fraud Unit. The Policy makers can develop appropriate policies and alternative actions based on empirical evidence and data.

1.5.4 Researchers and Scholars

The researcher gained experience in research and will use the results to detect, recommend and review existing policies revolving on operations in departments that are prone to fraud. Scholars will find the study useful as a source of knowledge and insight while others may use it for future research on the banking industry and the factors that motivate fraud in the banking industry.

1.5 Scope of the Study

This study was conducted using a sampling frame of all employees in the 17 branches within Nairobi County. The total population of the study was 650. In total there were 204 employees who formed the sampling frame. The data was collected during the months of January and

March 2014 using Commercial Bank of Africa (CBA) as the case study. This was done using a questionnaire between the 20th of February and 10th of March 2014.

The researcher encountered the following limitations in the course of the research: Data access limitations: information held by auditors about fraud was sensitive to the bank and was not easily available. This was countered by assuring the information providers of anonymity and confidentiality. Furthermore, confidentiality agreements with the respondents were arrived at during data collection.

1.6 Definition of Terms

1.7.1 Fraud

Fraud is a deliberate deception to obtain illicit material gain, and includes embezzlement and asset misappropriation (Pan *et al.*, 2011).

1.7.2. Control Systems

A control system consists of subsystems and processes put together for the purpose of controlling the outputs of the process (Ganesh A. and Raghurama, A., 2008).

1.7 Chapter Summary

This chapter has presented the background of the study including the fraud risks and challenges identified by PwC and CBK. This background informs the problem of the statement, research questions, and scope of the study and the importance of the study. Chapter two reviews the existing literature on banking fraud drawn from books, journals and dissertations. Chapter three presents the research methodology and design to be used in the research. Chapter four of the study presents the findings and interpretations from data collected and analyzed. Chapter five presents the discussion of findings, conclusions and recommendations of the study.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

As business becomes more complex and management strategists fret over slashing costs and boosting profits, employees are gaining additional opportunities to commit fraud. Recent trends towards downsizing, reengineering and corporate layoffs, and organizations have a very volatile workforce, often without much company loyalty. This environment is ripe for computer and employee fraud (Haugen, 1999). Banking fraud hurts both banks and their customers.

This chapter reviewed literature on the factors that cause fraud specifically in the banking industry. This was covered in three sections namely: the factors that cause fraud in the banking industry, the types of fraud and also preventive and control measures.

2.2 Factors that Contribute to Fraud in the Banking Industry

Fraud cannot be studied, examined or attributed to one factor only. On the contrary, a multifaceted and multifactor approach to the study of fraud must be undertaken. Looking at a fraudsters perspectives, it is necessary to take account of motivation of potential offenders, condition under which people can rationalize their prospective crimes away, opportunities to commit crimes, perceived suitability of targets for fraud , technical ability of the fraudster, the possibility and likelihood of fraud discovery and carrying out, expectations and consequences (job loss, family stigma and proceeds of crime confiscation and actual consequences of discovery (Chartered Institute of Management Accountants [CIMA] , 2009).

A research conducted by Kingsley (2012) in Nigeria revealed that institutional factors that lead to fraud may include but are not limited to weak accounting system control systems, inadequate supervision of subordinates, disregard of Know Your Customer rule, poor information technology and data base management, hapless personnel policies, poor salaries,

general frustration occasioned by management unfulfilled promises, failure to engage in regular call over, employees refusal to abide with laid down procedures without any penalty, banks reluctant to report fraud due to the perceived negative publicity, banking experience of staff and inadequate infrastructure that may include poor communication systems result to a buildup of unbalanced posting, inadequate training, poor book keeping and genetic traits like kleptomaniac who pathologically steals for fund (Kingsley, 2012) .

Social factors are those that can be traced to the immediate and remote environment which may include penchant to get rich quick, slow legal process, poverty widening gap, job insecurity, peer group pressure, societal expectations, financial burden on individuals, stiff competition in the banking industry may see banks engaging in fraud to meter up in terms of liquidity and profitability (Kingsley, 2012).

According to a survey done in 2009 by fraud examiners, the current increase in fraud cases stems from the intense pressure faced by individuals. According to the study, fraud grows and thrives under three major factors: pressure on employees to commit, availability of opportunities for fraud and the ability of the employee to rationalize the act of fraud (Pan *et al*, 2011). However, this factors may drive fraud under differing conditions and environments. The factors may lead to proliferation of fraud during economic hardships especially when the organization and or the employees are undergoing times of economic and financial strain. Similarly, as companies seek to reduce their level of employees or reduce their expenditure especially on employee allowances and remuneration, the opportunities for fraud may increase due to a reduction in the effectiveness of internal controls. This is infract grounded in the findings of the study of the Association of Certified Fraud Examiners (ACFE) (2009) in which over 80% of the respondents indicated that economic hardships was a reason for the growth of growth in fraud. Employee layoff has the effect of establishing gaps in the internal control systems which promote fraud. In effect the ACFE (2009) concluded that there exists an inverse relationship between fraud in the organization and its economic strength.

Trust in employees is also a driver of fraud in organizations. According to Cressey (1973) trusted employees can lead to increases in fraud especially where the guilty employees perceives to have a dilemma or financial problem which he/she deems not shareable with the management or fellow employees. If the employee genuinely believes that the violation of the trust may lead to the solution of the problem, the employee will most likely violate this trust and secretly resolve the problem (Cressey, 1973).

Insider theft has a significant negative impact on the profitability of the business. Existing statistics show that over 33% of all bankruptcies in businesses is primarily driven by employee theft. (Wang and Kleiner, 2005). However, this may not come as a surprise to the management which will have identified this through indicators such as rumors, inventory shortages, reduced earnings etc. Rationalization of the fraud act, poor internal controls, lack of implementation of laws and policies and managements indifference to the acts of fraud are major drivers of employee theft (Wang and Kleiner, 2005). In addition, employees argue that the management creates opportunities for fraud which is their primary motivator of fraud rather than their financial need. Furthermore, most employees believe that management inaction against fraud is a major driver of fraud in the organization (Wang and Kleiner, 2005). This means that if an organization/management expects a fraud free environment it must set examples through honesty, action and adherence to policies (Wang and Kleiner, 2005).

A red flag is a set of circumstances that is unusual in nature or vary from normal activity. It is a signal that something is out of the ordinary and may need to be investigated. Employee red flags include lifestyle changes (expensive cars, jewelry, homes clothes, and significant personal debt and credit problems) behavioral changes, high turnover especially in areas vulnerable to fraud, refusal to take vacations or sick leave and lack of segregation of duties in the vulnerable areas. A fraud model brings together all these aspects of fraud. According to ACFE (2009) his factors are embedded in a model grounded on three factors promoting fraud: motivation to fraud, availability of opportunities and rationalization of the act of fraud (ACFE, 2009).

2.2.1 Pressure to Commit Fraud

The pressure to commit fraud may emanate from different sources. Nonetheless, Wilson (2004) noted that greed in employees is the major sources of pressure. This relates to duress that is caused by an employee immediate need for assets (Cressey, 1973). Hillison *et al*. (1999) state that 95% of all fraud cases involve needs caused by financial difficulties or vice related activities. Pressure pushes the fraudster to take risks in order to obtain what they want. Notably, an emergency of finance is only seen from the view of the fraudster to the lead to act of fraud. The pressure may actually now even be seen by a third party observer. It is the combination of emergency and need that is common to the concept of pressure to commit fraud. Pressures are often not readily apparent from day to day activities, then fraud investigators need to gain knowledge and understanding of the employees and to consider types of pressures that prevail.

Hillison *et al*. (1999) found that numerous employee situations are consistent with actual or perceived pressure. For example: Greed or preoccupation with successful, living beyond one's means, high personal debts, high medical bills, poor credit or inability to obtain credit, unexpected financial needs, personal financial losses, expensive habits such as the use of drugs, alcohol or gambling, illicit sexual relationships, work related pressure such as low pay, failure to receive a promotion unfair treatment, lack of respect or dissatisfaction with one's job, boredom, challenge to see if you can beat the system without getting caught and spouse or family related imposed pressures (Hillson *et al.,* 1999).

Every fraudster faces some kind of perceived pressure most of which involve a financial need. There exists various non-financial pressures that can lead to fraud. Albrecht (2008) noted that when an employee is under pressure to perform, wants to display better than actual performance, is experiencing frustration at the work place or even has set challenges to beat the system, this are adequate motivators of fraud. Pressures perceived by one individual, such as a gambling addiction, may not be pressure to another individual. Some of the financial pressures that enhance and enable the proliferation of fraud are financial losses, falling sales,

failure to meet earnings expectation or inability to compete with other companies (Albrecht, 2008).

2.2.2 Opportunity to Commit Fraud

Opportunity is the first important factor motivating fraud. . Opportunities to commit fraud represent gaps, deficiencies, weaknesses and loopholes in the internal control systems of a business that an employee can utilize to commit fraud (Wilson, 2004). Hillison *et al*. (1999) found that opportunities to commit fraud can arise when an employee acquires absolute trust in an organization where the internal controls are weak or nonexistent. The employee will then perceive that an opportunity exists to commit fraud, conceal it and avoid detection.

Companies with weak internal controls are at higher risks of recording fraud cases and opportunities for fraud. According to CIMA (2009) where a business does not have adequate security over its assets and property and exposes the assets the likelihood of fraud is higher than otherwise. On the other hand despite the levels of honesty in employees (i.e. from total honesty to total dishonesty) the availability of opportunities may sway the employee into committing fraud.

Hillison *et al.* (1999) noted that strong internal control systems are an important means of limiting the opportunity for fraud but when controls exists, a person with unlimited access and overriding authority gained through trust may be able to override the controls to commit fraud. While auditors cannot readily regulate the pressure attribute, they can help mitigate opportunity to commit fraud. Typical failures in control related issues that increase opportunity for fraud include: lack of segregation of duties, failure to inform staff about company rules and the consequences of violating them, rapid turnover of employees, constantly operating under crisis conditions, lack of an audit trail, ineffective supervision, lack of transaction authorizations, poor accounting records, lack of physical controls, lack of access to information, breakdown of procedures. Employees attempting to commit fraud are likely to work unusual hours and do not take days off (Hillson *et al.,* 1999).

2.2.3 Rationalization of the Act of Fraud

Rationalization of the act of fraud also known as the moral justification through which employees create an attitude or thought that committing fraud is proper and right. It is created when an employee justifies his actions or crime through statements such as: it will be impossible for the company to find, the company can do without it, I am stealing, the company does not recognize my efforts and therefore it's my reward for hard work (Clark and Hollinger, 1983). This justification for the act of fraud often lead to fraud in the business. Justification of the acts of fraud can also emanate from the actions of superiors who engage in fraud. Junior employees will therefore engage with the rationalization that others are doing it, the earnings of the business are adequate to cover the losses or I am angry at the company (Clark and Hollinger, 1983). In summary Clark and Hollinger (1983) argued that most individuals commit fraud due to the consistency in the justification and the personal code of ethics.

Hillison *et al*. (1999) stated that for most, personal integrity may be the key limiting factor in keeping a person from misusing assets. That is, many employees would not commit fraud even if a need or opportunity arose. Many individuals observe the rules and regulation because they have faith in it and or are terrified of being humiliated or rejected by people they care about if they are caught. CIMA (2009) further notes that individuals may rationalize the act of fraud since they have they believe and perception that the victim is well cushioned or protected from the impact arising from the fraud or because the victim deserves it. Rationalization is personal to the person and more difficult to combat (CIMA, 2009).

In summary it is evident that employees attitude are modelled towards committing fraud due to perceptions of low remuneration, too much work and too little compensation, being at par with others who are committing fraud, perceptions that there is prestige and privilege in fraud, low self-esteem and respect, as an act of revenge, intuitions that it's only a loan and will be repaid and other justifications such as it will be paid, no one is getting hurt, it's for a good case or it's only a temporary alternative.

2.3 Types of Fraud

Fraud has been classified in various ways using various parameters: Management fraud, Insiders who are purely employees of the banks, outsiders who are customers or non-customers of the banks and insiders /outsiders, which is a partnership of the employees (insiders) and outsiders.

2.3.1 Management Fraud

This is frequently committed by management staff e.g. general managers, managing directors. The victims of this kind of fraud are investors and creditors and this is done via financial statements. Management fraud is driven by the need to acquire more resources from new and existing share capital holders or suppliers. Management fraud may also be driven by the need to create a good corporate image/standing of the business in the eyes of the regulator or supervisor e.g. Central Bank and Kenya Bankers Association.

Management in most organizations is perpetrated through two major avenues: deception and deprivation. Management can overstate its assets or and revenues or understate liabilities and or expenses. ACFE (2011) believes that it is carried out through fictitious revenues, timing difference, improper asset valuation concealed liabilities and expenses and improper or inadequate discourse (Kingsley, 2012).

2.3.2 Employee Fraud

Employee fraud often referred to as non-management fraud is primarily committed by the employees of the banks (Kingsley, 2012; Tchankova, 2002). Employee fraud is mainly characterized by cash theft from bank tills, forgeries of customers signatures with the intention of withdrawing monies from the customer account, opening and operating fictitious accounts and illegal transfer of funds to other accounts (Tchankova, 2002: Akinyomi, 2012: Kingsely, 2012).

Employee fraud can also be driven through illegal transfer of funds and assets, false balance crediting, opening, use and management of fictional accounts, claiming of overtime for hours not worked, fund diversion (tapping funds from interest into a suspense account) computer fraud via compromising log in credentials of an e-banking user (Akinyomi, 2012: Kingsely, 2012).

ACFE (2009), Kingsely (2012) and Akinyomi (2012) in their respective studies on fraud in the financial and banking sector noted that staff can also collude to misappropriate organizations assets e.g. cash, inventory customer information. Therefore banks must take into consideration the location, place and security of assets and the responsible employees for the assets. Common employee fraud schemes include employees creating and paying for non-existent goods and services, payment of invoices that are inflated or made up, presentation of inflated and fake credit notes, customer list theft and unlawful acquisition of proprietary information (Kingsley, 2012).

Bank staff that have access to tangible assets and the accounting systems that record and track the activities of an employee. However, technologically savvy employees can use the same systems to conceal their identities and theft. This is especially so when the staff establish fake vendor accounts and embed them in the master file to enhance payment processing. Furthermore employees can steal products or assets of the company and charge the same to the cost of sales which reduces the profitability of the company while asset sales and removal for asset list will reduce the asset of the company (AFCE, 2009). Given the transition to a service based, knowledge economy and more valuable assets of a bank are intangible e.g. customer lists and copy righted material. Intangible assets theft may include the unauthorized copying and use of software's and other intellectual property (AFCE, 2009).

2.3.3 Third Party Fraud

Frauds perpetrated by customers and non-customers of banks are outsider fraud. These may include the following:

2.3.3.1 Cheque Fraud

This is the oldest financial crime. It is the commonest method by which customers and the bank are defrauded. Counterfeit cheques not written or authorized by legitimate account holder, forged cheques where a stolen cheque not signed by account holder, or altered cheque where an item that has been properly issued by the account holder but has been intercepted and the payee and/or the amount of the item have been altered (Onkagba,1993).

Forgeries is one entrenched mode of fraud where employees forge and copy a customer's signature with the aim of withdrawing funds from the customer's account. The major target accounts for forgeries are targeted savings account, deposit accounts, current accounts or transfer instruments. Experience has shown that most of such forgeries are perpetrated by internal staff in partnership with outsiders with the employees providing sample signatures of the customers (Akinyomi, 2012).

2.3.3.2 Kitting

Kitting involves the use of the time that normally lapses between depositing and clearing a cheque to acquire authorized loans without any interest. The primary objective of kitting is to utilize funds and interest fees to conceal short term cash deficiencies and shortages or to acquire funds for personal use. Competition among banks encourages bank to make funds available before time in order to attract special business accounts (Onkagba, 1993).

2.3.3.3 Misrepresentations and Impersonation

Fraudsters make false statements and or submit falsified documents including rent rolls, lien waivers and financial statements to boost loan applications. They may also make fraudulent disbursement requests to receive loan proceeds. This fraud activity may occur across simple banks using multiple accounts by opening an account with false identification (Onkagba, 1993).

In impersonation and misrepresentation, the fraudster always assumes the identity of another individual with the goal of committing a fraud or dishonest activity. Impersonation may be done to acquire cheque books to commit fraud or acquisition of cheque leafs for fraud purposes. According to Akinyomi (2012) impersonation is particularly very successful where the outsider works in collaboration with an insider.

2.3.3.4 Counterfeit Securities

This occurs when a good quality instrument is forged and used as an alternative to the stocks or assets as security for a loan. The fraudster gets the funds and disappears before the bank notes the documents are counterfeit. Counterfeits are one of the oldest forms of crime which has proliferated due to the advancement of photographic equipment and tools which has helped criminals to produce counterfeit documents that are of high quality and resemble original documents. According to Onkagba (1993) counterfeit documents may be copied, forged or simply changed in its details e.g. dates, terms of payment or holder.

2.3.3.5 Money Transfer Fraud

Money transfer services refers to the movement of financial assets and resources from one account to another mostly the beneficiary account. Money transfer can occur through mail, telephone or at the counter, mobile phones or through other electronic systems. Money transfer fraud occurs when the beneficiaries detailed are changed or altered to reflect those of a different individual or beneficiary (Onkagba, 1993).

2.3.3.6 Clearing Fraud

Clearing fraud can be committed by substituting cheques to enable a fraudster divert funds to a wrong beneficiary. There is also suppression of cheques such that at the end of the time required to clear a cheque the bank gives value as like authorizing bank had accepted payment of the value of the instrument (Onkagba, 1993).

2.3.3.7 Letter of Credit Fraud

Letter of credit (also documentary credit) is a well-known payment method in international trade. This instrument has two fundamental principles: the autonomy or independent principle and the doctrine of strict compliance. Such principles intending to facilitate international transactions make letter of credit easy to be abused by fraudsters. Traders from developing countries who lack sufficient experience and knowledge of letters of credit are often the targets from an economic point of view; it is true that checking credibility involved information costs. It is better to incur the cost that the potential cost that would be involved if fraud were to occur. Apart from carefully checking the credibility of the seller beforehand, the buyer must cautiously choose suitable trade terms which allocate the risk of goods, cost, liability between buyer and seller (Zhang, 2013).

The Letter of Credit fraud occurs mostly in international trade where a supplier receives a spurious letter of credit, which is usually accompanied by bank drafts with fake endorsements which guarantees payments (Onkagba, 1993).

2.3.3.8 Card Fraud

This is committed at ATMS and posterminals. Fraudsters create a replica of a legitimate card or copying data contained in the cards magnetic stripe. Using this information, the criminals then use the cards (Onkagba, 1993). A fraudster can also use a giraffe method to monitor the information the customer keys into the ATM machine unknown to customers. A jammed ATM card can cause a customer to lose money. A fraudster pretending to be a genuine sympathizer will suggest that a victim reenter his or her security code. When the card holder leaves, the fraudster retrieves the card and reenters the code that he has doctored clandestinely. Fraudsters can also use data collected from tiny cameras and devices called skimmers that capture card information (Adeoti, 2011).

2.4 Prevention and Control of Fraud

Fraud risk is a contributor to the operational risks of a business. Operational risks refers to the errors and events in a transaction or process that put the assets of the business at risk. Some of the risks considered as operational risks include: incorrect and intentional false accounting, theft of assets or misappropriation of assets. Most banks focus on a limited number of risks mostly commonly of third party thefts but it's important to classify risks to possible type of offence and the potential perpetrators (Gates & Jacob, 2009).

It is important to assets fraud risk in each and every area of the business. However, special attention must be granted to high risk areas and departments such as cash and cash management, payments, sales and fixed assets. Management and acquisition of loans is also a key area of fraud risk management. As most researchers have found, fraud has a significant negative impact on the sustainability and profitability of a business. Businesses must therefore invest time and resources to the identification, management and control of fraud (CIMA, 2009). Further, existing studies have shown that the most effective methods of combating fraud include: reducing the motive of employees, enhancing internal controls thus reducing opportunities and ensuring that there is no justification of acts of fraud through proper supervision and implementation of rules and regulation plus punitive action against fraud (CIMA, 2009).

Kingsley (2012) noted that to reduce cases of fraud while enhancing the fraud detection and prevention strategies, businesses must have internal control systems embedded in the operational framework. Fraud in the banking sector and in deed in all businesses can be reduced if all control devices built into the system are implemented, enhanced and respected. Banks incur substantial operating costs by refunding customers' monetary losses (Gates & Jacob, 2009), while bank customers experience considerable time and emotional losses. They have to detect the fraudulent transactions, communicate them to their bank, initiate the blocking and re-issuance or re-opening of a card or account, and dispute the reimbursement

of their monetary losses (Douglass & Malthus, 2009). It is therefore in a bank's self-interest to put measures to prevent fraud or detect it as soon as it happens

An anti-fraud strategy includes elements of prevention, detection, deterrence and response. Business must develop concise and clear strategic responses towards fraud. This will include effective communication on the seriousness of fraud and the probable punitive measures taken due to fraud in the business. Identified cases must form case studies and examples of the stern action taken by the business against fraud. This is one of the most effective ways to combat fraud in the organization (CIMA, 2009).

2.4.1 Creating an Encouraging Work Atmosphere

Positive and good working environments enhances the compliance of employees to established rules, policies and procedures which are set for the success and sustainability of the business. A good working environment enhances communication between employees and management and guarantees positive employee recognition and great reward system. This kind of working atmosphere reduces the levels of internal fraud in the organization (Kingsley, 2012). A workforce culture includes having adequate and sufficient policies, rules, regulations, procedures, protocols and practices human resource management of employees (recruitment, selection, orientation, development, remuneration, career advancement, motivation, training and termination) to deter fraudulent and corrupt behaviors include practices that deal swiftly with incidents and protect whistle blowers (ACFE, 2009).

2.4.2 Ethical Culture

An ethical culture includes defining principles and values have indicators of high levels of ethics in the organization as well as zero tolerance to corruption and fraud. It also enhances ethical climate and mental notes in the employees not to engage in fraud and corrupt activities. Ethical culture should be incorporated via ethical leadership through rewards and acknowledgement as a model of appropriate conducts in the face factors and behaviors that would promote or motivate employees to engage in fraud (ACFE, 2009).

Attitudes within an organization often lay the foundation for a low or high risk fraud environment. In a high risk environment, petty issuers, expense fraud and other minor forms of fraud are overlooked or dealt with leniently. In low risk fraud environment, the business takes serious action on minor or major acts of fraud. In some cases, there may even be risk of total collapse of the organization either through a one act of fraud or very many small acts of fraud. Organizations have come to realize that high ethical standards bring long term benefits as customers and the community realizes that they are dealing with trustworthy organizations. They have also realized that improper, adverse actions, fraud and corruption often cause serious negative impacts to the people and organizations concerned when exposed (CIMA, 2009).

2.4.3 Types of Employees

Cost of hiring dishonest employees cannot be calculated: A dishonest employee will destabilize any effort to build a positive work atmosphere and constantly strive to defeat any internal measures. Companies should ensure they conduct a background check that covers criminal history, education, previous employment, civil history for possible lawsuits before employing anyone. The need to hire honest staff cannot be overemphasized (Kingsley 2012).

Fraud and business risk in any organization is inherent in the hired employees especially in senior positions where trust and authority are critical. Therefore it is crucial to conduct due diligence on employees and know them in order to authenticate their competence and credentials. Furthermore, this is important in knowing the integrity of the employee and how this will influence his actions in the organization. Employee due diligence can be undertaken through confirmation of education qualification, work experience and history and follow up with the references provide. In addition, due diligence may be crucial in acquiring undisclosed information by the employee especially one that may have an impact on the integrity of the employee (ACFE, 2009).

In undertaking employee due diligence, the business must take into consideration the applicable rules and regulations. This is because the rules and regulations will guide the conduct and acquisition of the information. Nevertheless, the business can acquire background information of the employee through authorized criminal record survey. Other strategies to acquire information about an employee include acquiring legal counsel on how to conduct and acquire employee information. Due diligence should also be undertaken on bank customers, suppliers and partners to identify any information with an impact on the financial health, ownership, reputation and integrity which may possess an unacceptable levels of risk (ACFE, 2009).

Bierstaker, Brody and Pacini (2006) found that it is important to note that an employee with fraud schemes may move from one organization to another. When employee records are not checked, dishonest people may be hired. An organization should not rely on telephone numbers listed on the resume for prior employers as they may be false. A company should try obtain employer telephone numbers independently. Organizations should also conduct a second reference check six months after an employee starts work. This is because for a dishonest employee, may have not been filed at the time of the initial search. This may be discovered by a second check.

2.4.4 Perform Expected and Unexpected Audit

Unannounced financial audits and fraud assessments should be done regularly. This can help unearth any vulnerability and appraise the effectiveness to the existing controls (Kingsley, 2012).Hillison *et al*. (1999) found that surprise fraud audits have potential to act as a deterrent to employee fraud. A surprise audit gives perpetrators less time to alter, destroy or hide records and other evidence. Some firms may be reluctant to use surprise, preemptive fraud audits because of a perception of adverse employee reactions. Honest employees should be made to understand the importance of fighting fraud. It may be important for management to periodically communicate to employees the importance of audits and also to

solicit staff input on how to conduct surprise audits. This may help in reducing suspicion and facilitate co-operation.

2.4.5 Enforce Internal Controls

This is designed to promote operational efficiency, provide dependable financial statistics, protect the assets and records and encourage adherence to prescribed policies. A sound internal control system have features that promote efficiency and effective tracking of transactions and ensuring that all activities are properly authorized, recorded, and reconciled (Kingsley, 2012).

An internal control system should have all principles and procedures that support the organizations effective and effective operation. They deal with things like approval and authorization procedures, restrictions and control over transactions, reconciliation of activities and accounts and provision of security to assets. The number of internal controls that an organization can have depends on nature and size. Internal controls minimize fraud. Examples of such controls may include requirement of multiple signatures for high value transactions, restriction belongings that can be brought into an office and conducting random searches.

As part of the risk management framework, the organization must review the internal controls and ensure that any weaknesses in the internal controls are addressed. Furthermore, the organization has the responsibility of ensuring that internal controls are assessed and updated to meet global trends and best practices constantly. This will reflect good practice. Finally, these internal controls should be entrenched within the organization culture and operations (CIMA, 2009).

2.4.6 Compensation Programs

It is a human trait to want recognition and reward for positive performance and success. Continuous and rigorous assessment of employees performance, coupled with constant,

timely and effective communication to the employee on the performance assessment has a huge bearing on the reduction of fraud. As part of the employee assessment process the organization must recognize and if possible reward any accomplishments of the employees, especially those whose performance require so. Furthermore, employees must feel that the reward is of value to them. Failure to do so will lead to guilt feelings, low motivation and demoralization of employees which might create rationalizations for acts of fraud.

Market research and surveys must also be done by the organization to identify whether the remuneration and compensation of employees is adequate, motivating and in line with industry trends. The findings of the survey will also be instrumental in striking a balance between the use of fixed and variable compensation. It is good to note that if compensation is based on compensation for short term performance, managers maybe motivated to cut corners or fabricate financial results to achieve those bonuses (ACFE, 2009).

2.4.7 Establish a Fraud Policy

Every bank should have an approach to deal with fraud. The approach should be clearly stated in the fraud policy. This is established to facilitate the implementation and actualization of internal controls which will aid in detection and prevention of fraud against companies. The must be applicable to any wrongdoing, or suspected misdeed, involving all stakeholders in the business (ACFE, 2009).

A fraud policy should have a scope, what actions constitute a fraud, the unit responsible for investigations, confidentiality clauses, and an authorization for investigating suspected fraud, reporting procedures, and termination procedures. A bank fraud policy should be separate and distinct from a corporate code of conduct or ethics policy. It should be clearly communicated to all employees through new orientation of new hires, annual training seminars and annual performance evaluations. It is important to have a written acknowledgement by each employee that the policy has been read and understood as required as stated by (Hillison, Pacini and Sinason, 1999).

2.4.8 Establishing a Telephone Hot Line

CIMA (2009) notes that a dedicated and confidential 24/7 hotline to report fraud is one of the most effective strategies to combat fraud. The hotline must be strictly confidential and will greatly aid the company's efforts to detect fraud. Indeed, studies have shown that most losses in an organization are caused by the ignorance of small signs and lack of fraud detection strategies. In addition to installation of a telephone hotline, every member of the organization must be aware that it is his/her responsibility to report any kind of fraud or irregularity in the business. Therefore, the hotline must have inbuilt facilities that ensure that the identity of the reporter is not revealed whether by choice or default (CIMA, 2009).

Anonymous tips received through hotlines are an effective strategy and channel to detecting fraud. The hotline should be utilized to create awareness, ensure ease in use and prompt actions on reports on the hotline. Education of employees on the use of the hotline is also important since they are the source of information.

To enhance the efficiency of the hotline it must be manned by a qualified and experienced employee who has multilingual abilities and is available 24 hours a day, 365 days a year. Once a fraud has been reported via the hotline, it would be important to let the whistle blower know that timely action will be taken. It would be important to analyze collected data against the industry norm. Hotlines may be supported in-house or provided by a third party (ACFE, 2009).

Bierstaker *et al*. (2006) found that some companies offer third party hotline service where a bank can subscribe. The annual subscription rate may be quite modest. The results of all calls are provided to the client within two or three days. A hotline may not be an effective detection tool but it enhances deterrence. Potential perpetrators will likely have second thoughts when considering the risks of being caught.

2.4.9 Enforce Mandatory Vacations

A mandatory vacation policy is used to insure banks. The policy requires that all officers take two consecutive weeks of vacation per year. It is important that vacations include an employee's high risk tasks. Job rotation programs should also be designed so that employee has little or no access to the documents, journals, data files, programs and other items that he has worked with on previous job. Mandatory vacations and job rotations plans deter fraud as well as allow existing frauds scheme to surface (Hillison *et al*, 1999).

2.4.10 Protect Information Systems

A fraud using or against an information system may be through entering false or fraudulent data into an information system or alteration of computer programs or code. One can program the computer to round off shillings and cent amounts down and accumulate fractions of cents in an account to which the fraudster has access. One can also steal data from an information system e.g. bank customer lists, merger plans etc. Computer fraud has increased because of the growth of internet which has increased the dial –in ports to computer networks. Although passwords are the oldest line of computer defense, they still constitute the most effective and efficient method of controlling access. Proper password use is necessary if control is to be maintained (Bierstake *et al.,* 2006).

Employees in the bank should always ensure they change the default assigned passwords such as their last names to a more secure one. Employees should also be prohibited from sharing passwords with other users. Password security requires that they can be changed periodically (Bierstake *et al.,* 2006).

An organization operating system should keep track of unsuccessful attempts to gain access and limit attempts before the user is automatically signed off according to Hillison *et al.* (1999).Technology has advanced to create new forms of passwords protection using biological features of the user such as voice prints, finger prints, retina patterns and digital signatures (Bierstake *et al.,* 2006).

2.4.11 Increase the Use of Analytical View

Bierstake *et al*. (2006) found that increase the use of analytical view can assist to prevent and detect fraud. Fraud can affect financial statement trends and rations. Accounts may therefore be manipulated to conceal a fraud. It may be important for an investigator to analyze several years of financial statement data to obtain a clear picture of the financial impact of the crime if any. Fraud analysts should check for erratic patterns in account balances. If present it means there is a fraudulent activity.

2.5 Chapter Summary

This chapter has reviewed the existing literature on fraud in the banking sector across the world. The literature is reviewed from international journals, dissertations and books. Nevertheless, most of the literature is available for review and is drawn from experiences in America, Europe and West Africa. The lack of empirical evidence in the East African region and specifically in Kenya creates a huge literature gap as empirical evidence from West Africa especially Nigeria cannot be used to generalize bank fraud in Africa due to differing environmental factors.

The major critic of reviewed literature is that is drawn from developed financial markets and institutions with well entrenched policies and systems to detect and combat fraud. On the other hand, the lack of literature on the Kenyan scene makes it very hard to provide evidence to the existence and prevalence of various types of fraud in the banking sector. However, this is not to dispute that banking fraud is present in Kenya, since statistics from the CBK (2013) indicate growing cases of bank fraud. This research seeks to address the shortage of empirical data on banking fraud in Kenya.

Chapter three below presents the research methodology to be used in the study. It presents the research design, population and sampling techniques, the data collection and analysis techniques.

CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 Introduction

This chapter provides further information on the research design method used in determining the area under study. In addition, it highlights on thepopulation under review, sampling technique, data collection method, and research procedure and data analysis method.

3.2 Research Design

Orodho (2008) defined a research design as the blue print of the study that provides the outline and direction of a research. This study used a descriptive research design using a case. A descriptive research design involves the investigation of a topic with the aim and purpose of describing the problem or identifying problems (Kothari, 1985). A descriptive research design was justified for use in this study as it sought to identify and describe how the independent factors influenced the dependent variable. The independent variables were: Types of fraud, causes of fraud and mitigation measures in place and how this influenced fraud in the banking industry.

The case for this study was the Commercial Bank of Africa (CBA). Commercial Bank of Africa was used in this study as it was one of the largest banks in Kenya, with the largest number of personal accounts in the country (CBK, 2013; KBA, 2013). Furthermore, most of frauds in the world occur online i.e. through the use of information communication technologies (Akinyomi, 2012). Since CBA had the most successful mobile banking platform in Kenya (M-SHWARI), its inclusion in this study enhanced the validity of findings. Finally, CBA was used as the case of the research to ease of data collection by the researcher.

3.3 Population and Sampling Design

3.3.1 Population

Population is defined by Cooper and Schindler (2001) as the total collection of elements about which we wish to make some inferences. The population includes all groups with the same attributes. The population of this study was drawn from all employees working in Commercial Bank of Africa (Kenya). In total there were650 employees working in various branches across Kenya (CBA, 2013). Employees working within Nairobi County (location of the study) were 204 who comprised the population of this study.

Table 3.1: Population

Class of employee	Number in each branch	Number of Branches	Total population	Percentage
Branch Managers	1	17	17	8%
Middle Level Managers	4	17	68	34%
Auditors/Risk Managers	1	17	17	8%
Clerks	6	17	102	50%
Total			**204**	**100%**

Source: CBA (2013)

3.3.2 Sampling Design

3.3.2.1 Sampling Frame

A sampling frame according to Cooper and Schindler (2001) is a list of elements in the population from which the sample is actually drawn. The study was undertaken in all CBA branches in Nairobi County. The sampling frame was drawn from various employees in CBA as shown in Table 3.1 above.

3.3.2.2 Sampling Technique

Sampling techniques refers to all the systems and process that a researcher uses to select the sample size (Cooper and Schindler, 2001). This study used a stratified random sampling technique. A stratified random sampling technique was justified for use in this study as it was based on scientific rules of probability, ensured adequate representation of all classes of employees and reduced the probability of respondent bias in the study i.e. respondents predominantly selected from one class. The stratums for this study were derived from the various employee classes who had a direct involvement in identification, prevention and reporting of fraud. The strata's were: branch managers, middle level managers, auditors and risk managers and clerks.

3.3.2.3 Sample Size

The sample size of a statistical sample can be defined as the number of observations that constitute it (Yin, 2003). Taking into consideration variables such as homogeneity in the data, and the experiences of other researchers (Bierstaker *et al*., 2006), this study utilized a sample size of 68. The use of 68 respondents in the study was justified as it was in line with the recommendations of Mugenda and Mugenda (2003) who indicated that a descriptive study should include at least 30% of the total population. Since the sample size of 68 represented 33% of the population it was deemed appropriate. Furthermore, the sample size allowed the researcher to collect data from respondents across the various branches and offices of the bank. The distribution of the sample size was as shown in Table 3.2 below.

Table 3.2: Sample Size

Class of employee	Sampling Frame	Sample Size	Proportion
Branch Managers	17	17	100%
Middle Level Managers	68	17	25%
Auditors/Risk Managers	17	17	100%
Clerks	102	17	17%
Total	**204**	**68**	**33%**

NB: This distribution indicated one respondent for each of the classes in each employee class

3.4 Data Collection Methods

This research used primary data. Primary data for this study was collected using questionnaires. The questionnaire had open-ended and closed-ended questions. The questionnaire format was in three sections. First section had bio data and general questions. Second section had open ended questions regarding causes of fraud and a likert scale on staff awareness of fraud management culture. Section three sought to find out if the current risk management and fraud prevention processes at CBA had been effective and this was on a likert scaling measurement tool which also enabled the researcher to objectively rank the responses. The method of data collection was used in a fraud research by Bierstaker *et al*. (2006) and they confirmed that it did not affect the statistical significance of the results at conventional levels.

3.5 Research Procedures

The questionnaire developed was pretested with five CBA staff. This assisted to detect weaknesses in design and instrument. A pre-test had been seen to save researchers from disaster by using suggestions of the pre-test group to change confusing, awkward or offensive questions.

The actual research was then conducted after incorporating feedback given by the pre-test group. The primary data was collected through internet questionnaires based on research question. Data was collected by e-mailing the online questionnaires link to staff in the selected CBA branches with the respondents expected to complete the questionnaires online. Respondents were not required to give their personal details to ensure confidentiality and anonymity. To ensure a high response rate, the respondents were first contacted on phone. Reminders were also sent a week after the questionnaire was distributed to those who had not attempted the questionnaire.

3.6 Data Analysis Methods

Once the data was received, the researcher edited the data by checking for missing data or unfilled sections of the questionnaire. Only sections properly filled were used. After cleaning and editing of data, coding was done in the statistical software. The statistical software used to analyze data collected was SPSS (Statistical Package for Social Sciences) due to its ease of use.

The collected data was analyzed using mean and mode which were measures of central tendency. Other data analysis techniques and measures used in this study included: range, standard deviations and variances. To analyze particular responses of the different classes of respondents cross tabulation was undertaken. Correlation analysis was also undertaken to investigate the relationship between various contributing to fraud in banks. Final data analyzed was presented using tables, figures and frequency distributions.

3.7 Chapter Summary

This chapter presents the research methodology of the study. It shows the research design, data collection, population and sampling techniques and data analysis processes adopted. Chapter four presents the findings and results of data collected and analyzed.

CHAPTER FOUR

4.0 RESULTS AND FINDINGS

4.1 Introduction

This chapter presents the findings of the study on fraud in the banking sector. The findings are deduced from the data collected, analyzed and presented in this chapter. In total, 60 responses were used for analysis representing an 89% response rate from the respondents.

4.2 Background Information

This section presents the background characteristics of the respondents.

4.2.1 Gender

Seventy percent of the respondents to this study were of the male gender, while 30% were of the female gender. These findings imply that the population of study was characterized by a higher proportion of the male than the female gender. This is as shown in Figure 4.1 below:

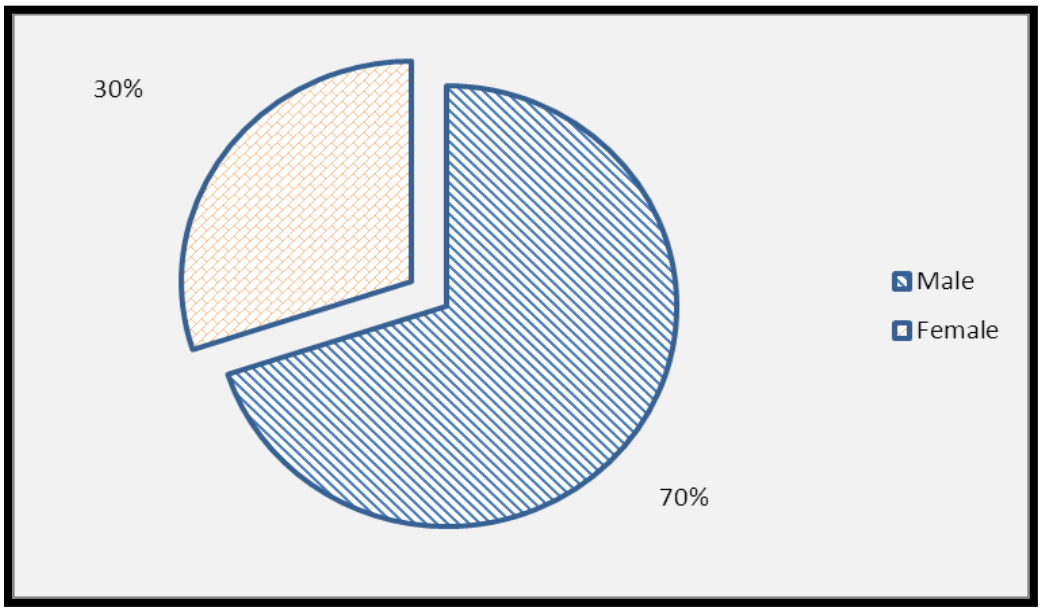

Figure 4.1: Gender of Respondents

4.2.2 Age

The respondents to this study were spread out across various age brackets. However, the 18 – 29 age bracket represented the biggest proportion of respondents (60%). Respondents between the ages of 30 – 49 were 33% while those of the ages between 49 and 60 were 7%. This is as shown in Figure 4.2 below:

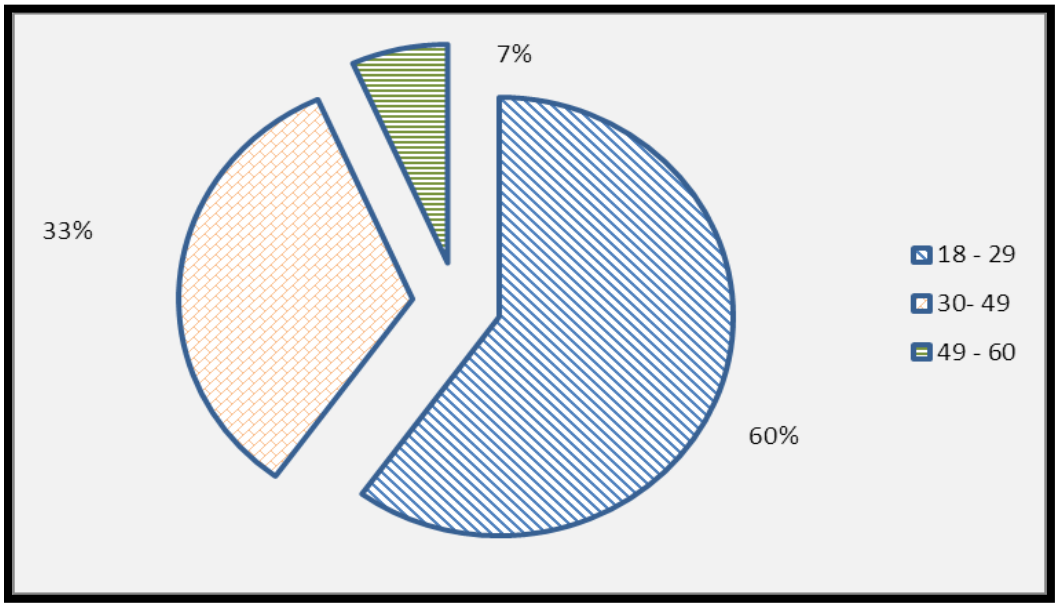

Figure 4.2: Age of Respondents

4.2.3 Role

Majority of the respondents to this study were risk managers/auditors (40%). Furthermore, 25% of the respondents were operational assistants/clerks, 22% were assistant managers and supervisors while 13% were senior managers. These distributions of respondents ensure validity of findings since the auditors (representing the largest proportion of respondents) are responsible for the detection and reporting of frauds.

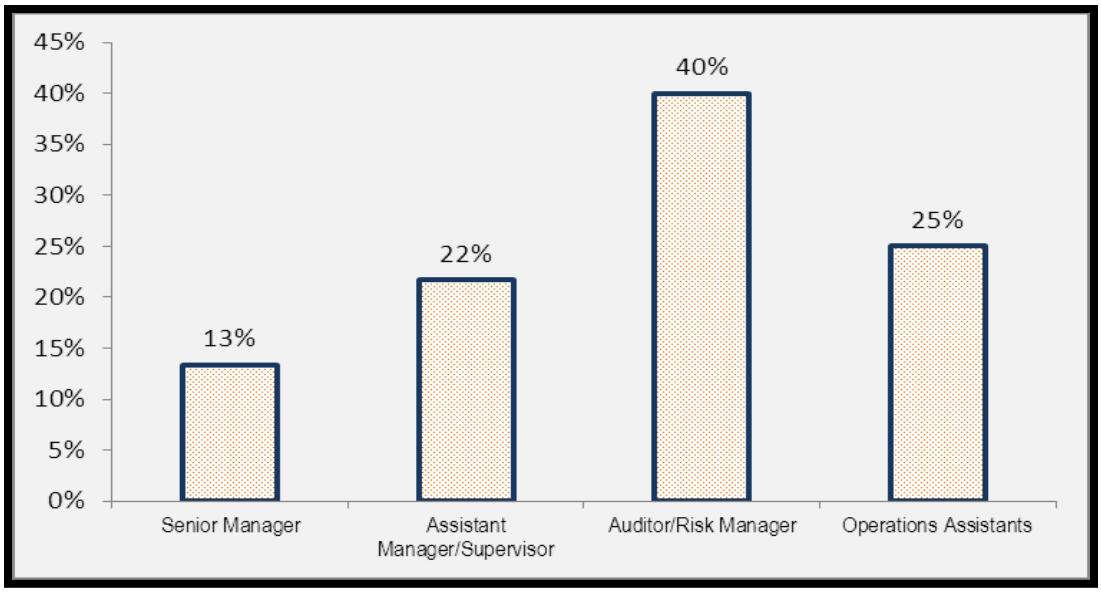

Figure 4.3: Role of Respondents

4.2.4 Experience

Sixty seven percent of the respondents to this study had an experience of less than 4 years, 20% had experience of between 5- 10 years while 13% had experience of over 10 years. This is as shown in Figure 4.4 below.

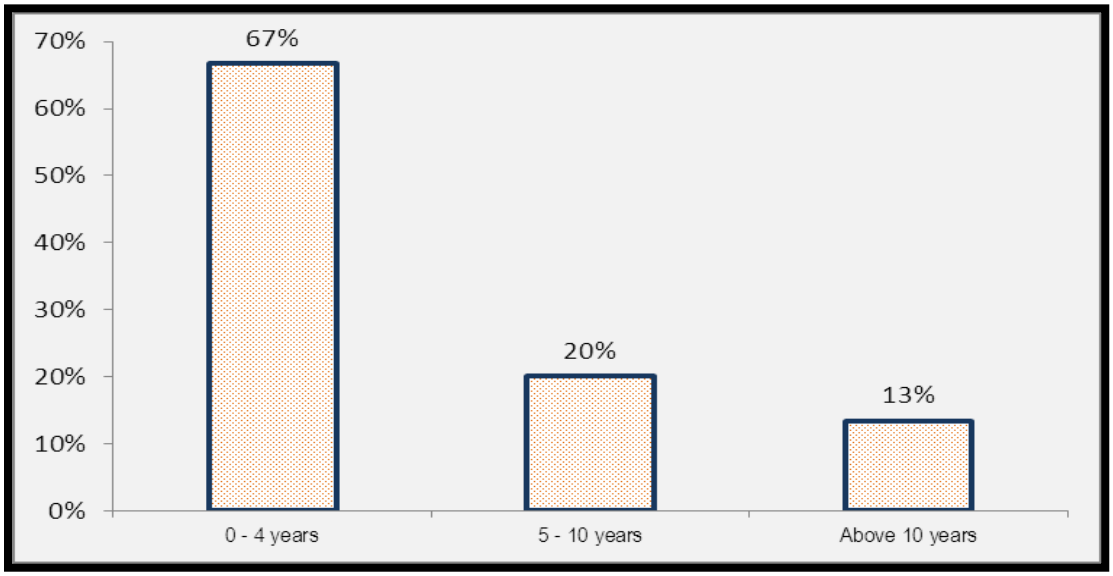

Figure 4.4: Experience of Respondents

4.3 Factors Contributing to Fraud

This section presents the findings of the study in relation to fraud in CBA.

4.3.1 Fraud in CBA

Fraud in CBA is accorded very high importance by the management. According to this study, 83% of the respondents indicated that very high importance is attached to fraud when it occurs while 17% indicated it was accorded average importance. This implies that fraud is critically managed and controlled in CBA.

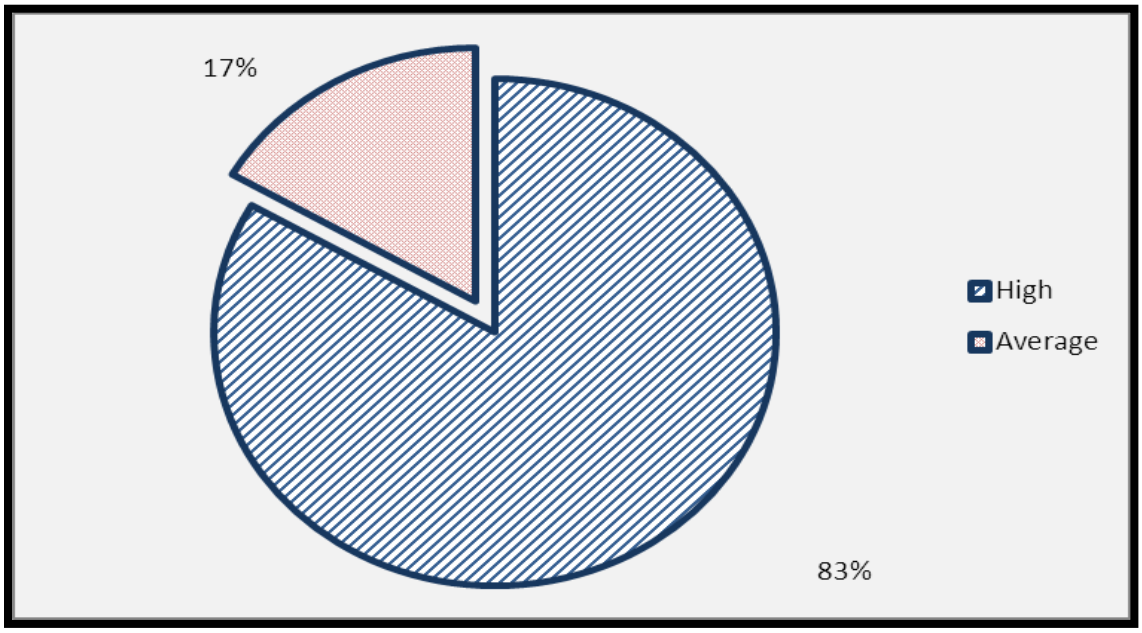

Figure 4.5: Fraud in CBA

4.3.2 Responsibility for Fraud

According to the 44% of the respondents, fraud analysts have the primary responsibility of detecting and controlling fraud. Thirteen percent of respondents indicated that it was the responsibility of the risk analyst while 42% indicated that it was the role of the auditor. This implies that the fraud analyst and auditors had the primary responsibility for fraud detection and control.

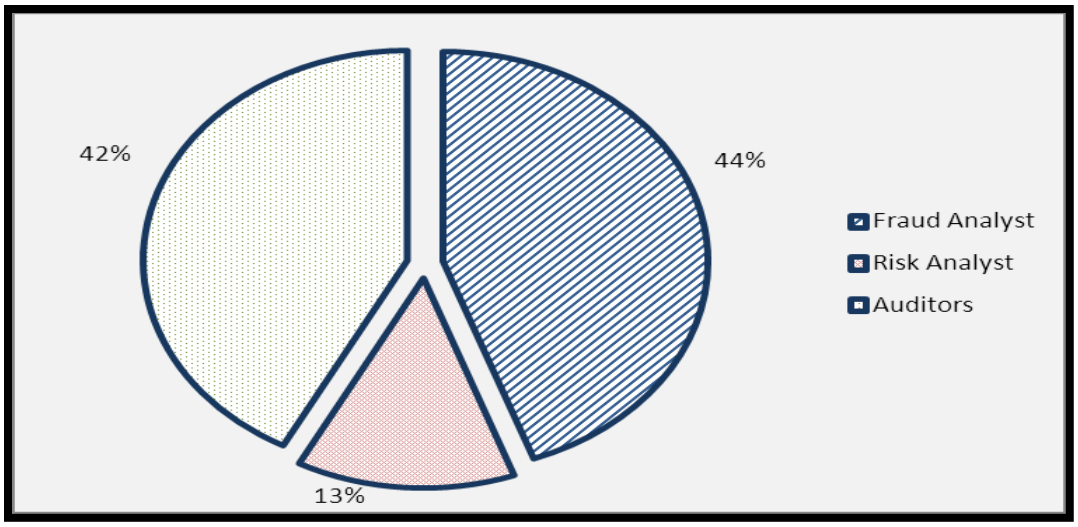

Figure 4.6: Responsibility for Fraud

4.3.3 General Causes of Fraud

The most common cause of fraud in CBA is the availability of opportunities to commit fraud. Pressure to commit fraud was the least common cause with a mean rating of 2.64 while rationalization of fraud acts had a mean of 2.12 as shown in Table 4.1 below. This implies that the availability of opportunities to commit fraud motivated most employees to engaging in fraud.

Table 4.1: General Causes of Fraud

	Pressure to Commit		**Rationalization of Act**		**Opportunities to Commit**	
	Frequency	**Percentage**	**Frequency**	**Percentage**	**Frequency**	**Percentage**
High	6	10	6	10	36	60
Average	6	10	42	70	18	30
Low	48	80	12	20	6	10
Mean	2.64		2.12		1.47	
Mode	3		2		1	
Standard Dev.	0.314		0.247		0.184	

4.3.4 Weak Internal Controls and Accounting Systems

According to 40% of the respondents, weak internal controls and accounting systems had a very high contribution to fraud in the bank. Thirty percent of the respondents indicated it had an average contribution while 30% indicated that it had a low contribution. This implies that weak internal controls and accounting systems had significant motives to fraud by employees.

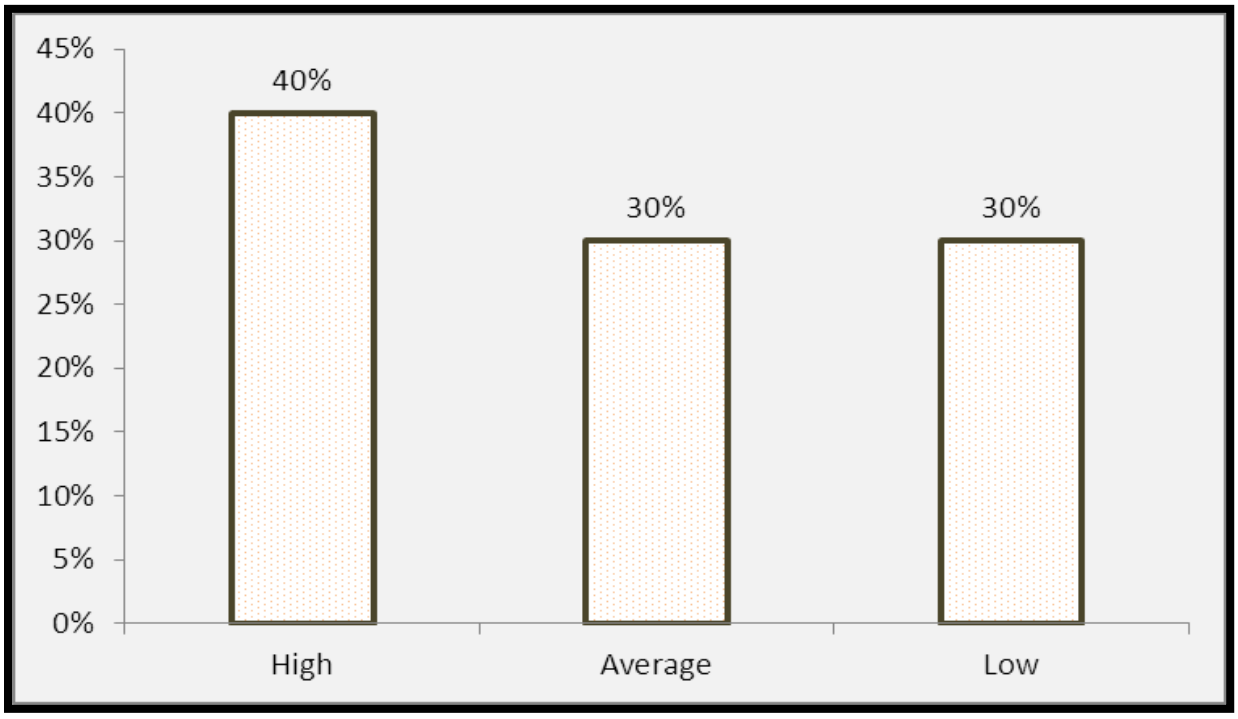

Figure 4.7: Weak Internal Controls

4.3.5 Inadequate Supervision of Subordinates

Inadequate supervision by subordinates had an intermediate contribution to fraud in CBA. This is according to 50% of the respondents in the study. Further, 30% of the respondents indicated that it had a high contribution while 20% indicated that it had a low contribution. This shows that supervision was lacking and motivated most employees to engage in fraud.

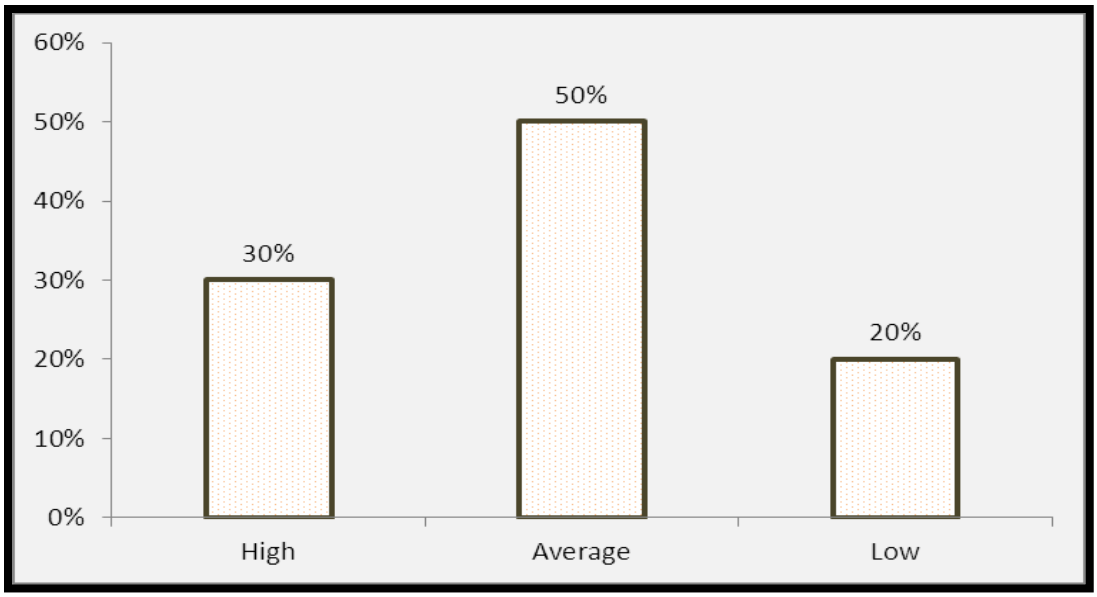

Figure 4.8: Inadequate Supervision of Subordinates

4.3.6 Disregard for Customer Knowledge Rules

Forty percent of the respondents indicated that disregard for customer knowledge rules (Customer due diligence) led to fraud to a high and average extent. Further, 20% of the respondents indicated that it contributed to fraud to a low extent. This denotes that the lack of customer knowledge in the bank led to fraud thought this was to a high extent.

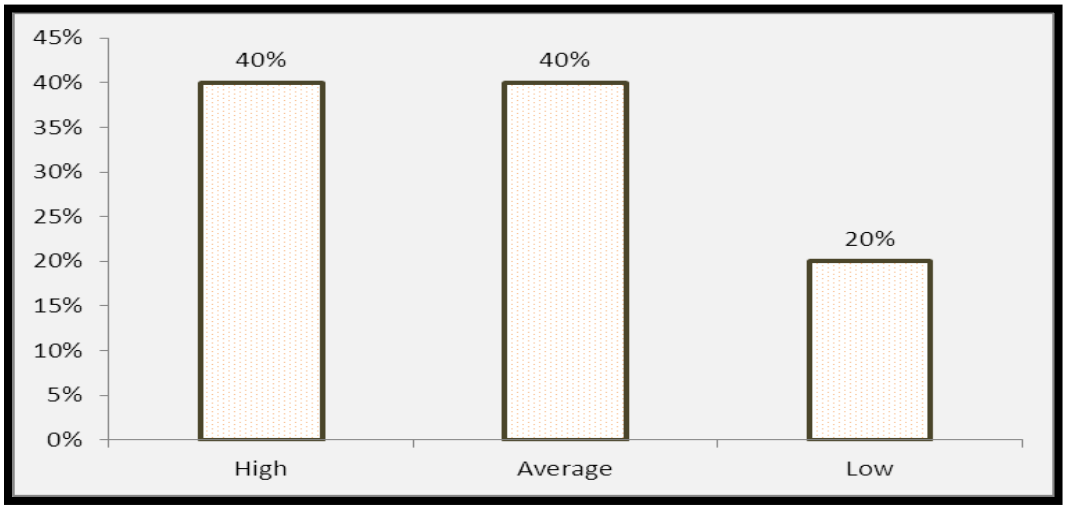

Figure 4.9: Disregard for Customer Knowledge Rules

4.3.7 Poor IT Structures

According to 40% of the respondents, poor IT structures contributed highly to fraud in CBA, 33% indicated to a moderate extent while 27% indicated that it contributed to a low extent. This implies that poor IT structures led to fraud to a high extent in CBA.

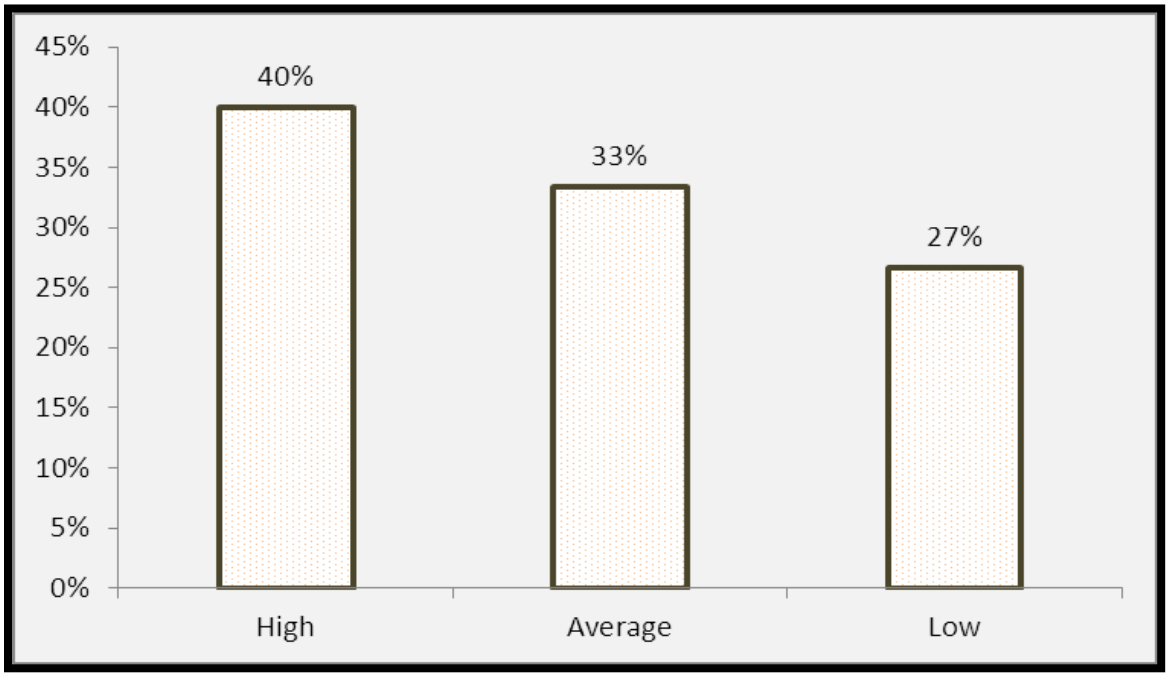

Figure 4.10: Poor IT Systems

4.3.8 Poor Personnel Policies

Poor personnel policies led to fraud to a moderate extent. This is deduced from the findings of this study. Seventeen percent of the respondents indicated that poor personnel policies led to fraud to a high extent, 50% indicated that it led to a moderate extent, 20% indicated that it led to a low extent while 13% indicated that poor personnel policies did not have an impact on fraud. These findings imply that CBA had adequate personnel policies to deter fraud.

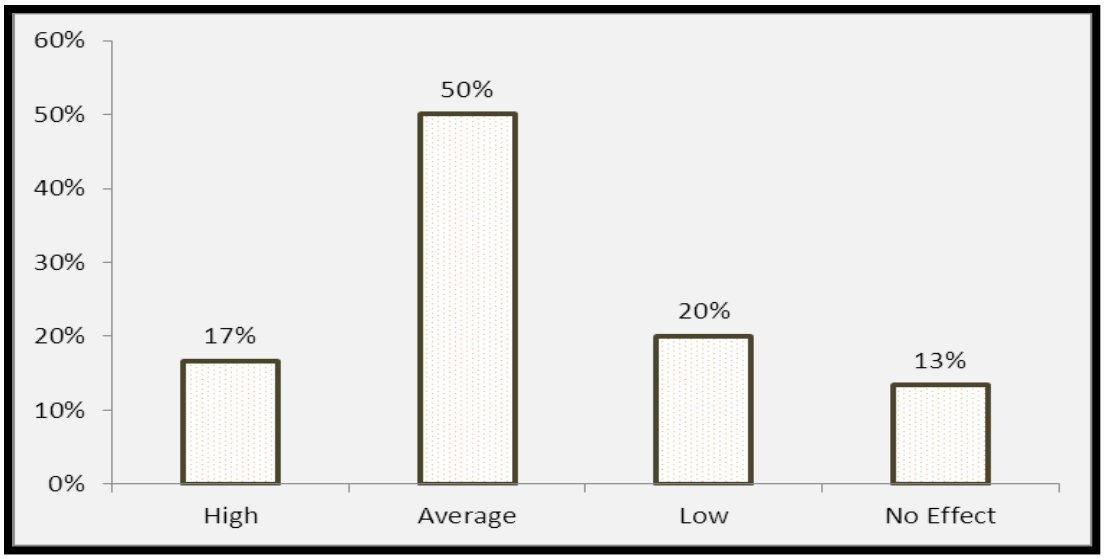

Figure 4.11: Poor Personnel Policies

4.3.9 Low Remuneration of Employees

To a moderate extent, low remuneration of employees led to fraud in CBA. According to 33% of the respondents, remuneration contributed to fraud to a high extent, 52% indicated that it led to a moderate extent, 10% indicated it led to fraud to a low extent while 5% indicated that it had no impact. This implies that remuneration levels were relatively high in the bank discouraging the need for fraud.

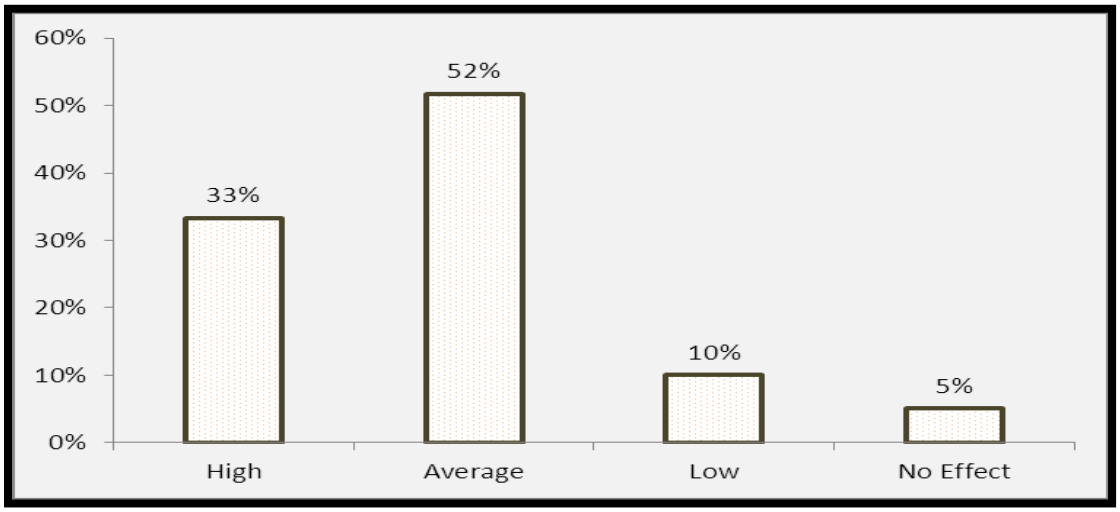

Figure 4.12: Poor Remuneration of Employees

4.3.10 Correlation Analysis of Causes of Fraud

This study sought to investigate the relationship between the various variables causing fraud in banks. The correlation analysis using the pearson correlation statistic show that the opportunities to commit fraud and rationalization of the act of fraud had a negative correlation (-.415) which was significant at 0.01 significance levels. Weak internal controls had a positive correlation to opportunities to commit the fraud crime (.269) which was significant at 0.05 significance levels. Inadequate supervision had a negative correlation with pressure to commit (-.543) significant at 0.01 levels, rationalization of the act (-.504) significant at 0.01 levels and a positive relationship with opportunities to commit crime (.319) significant at 0.05 levels and weak internal controls (.499) significant at 0.01 levels.

Disregard of customer knowledge rules had correlation of -.543, -.447,.611 and .916 which were significant at 0.01 significance levels to pressure to commit, rationalization of the act, opportunities to commit and weak internal controls.

Poor IT structures was negatively correlated to pressure to commit (-.543) and rationalization of the act (-0.447). On the other hand, IT structures had a positive correlation to weak internal controls (0.611), and inadequate supervision (0.916) all of which were significant at 0.01 significance levels.

Poor Personnel Policies were correlated to pressure to commit (-0.423), rationalization of the act (-0.504), inadequate supervision (0.852) and disregard of customer knowledge rules (0.870) at 0.01 significance levels. Similarly, poor personnel policies were correlated to weak internal controls (0.326) at 0.05 significance levels.

Low employee remuneration was correlated to rationalization of the act (-0.682), opportunities to commit (0.342), weak internal controls (0.304), inadequate supervision (0.852), customer knowledge rules (0.828), poor IT structures (0.828) and poor personnel policies (0.871) at 0.01 significance levels.

These findings imply that the factors that greatly lead to increase in fraud in the banking sector since they had a strong positive correlation were: inadequate supervision and weak internal controls, disregard of customer knowledge rules and inadequate supervision, poor IT structures and disregard of customer knowledge rules, poor IT structures, poor supervision, poor personnel policies and inadequate supervision, poor personnel policies and disregard of customer knowledge rules, poor employee remuneration, inadequate supervision, disregard of customer knowledge rules and poor IT structures. These were the major factors leading to an increase in the occurrence and frequency of fraud in the banking sector. The Correlation analysis is as shown in Table 4.2

Table 4.2: Correlation Analysis

		Pressure to Commit Fraud	Rationalization of Act	Opportunities to Commit Fraud	Weak Internal Controls	Inadequate Supervision	Disregard of Customer Knowledge rules	Poor IT Structures	Poor Personnel Policies	Low Remuneration
Pressure to Commit Fraud	Pearson Correlation	1	.087	-.116	-.244	-.513**	-.543**	-.543**	-.423**	-.251
	Sig. (2-tailed)		.509	.376	.060	.000	.000	.000	.001	.053
	N	60	60	60	60	60	60	60	60	60
Rationalization of Act	Pearson Correlation	.087	1	-.415**	.022	-.504**	-.447**	-.447**	-.504**	-.682**
	Sig. (2-tailed)	.509		.001	.865	.000	.000	.000	.000	.000
Opportunities to Commit fraud	Pearson Correlation	-.116	-.415**	1	.269*	.319*	.199	.199	.081	.342**
	Sig. (2-tailed)	.376	.001		.038	.013	.127	.127	.539	.007
Weak Internal Controls	Pearson Correlation	-.244	.022	.269*	1	.499**	.611**	.611**	.326*	.304*
	Sig. (2-tailed)	.060	.865	.038		.000	.000	.000	.011	.018
Inadequate Supervision	Pearson Correlation	-.513**	-.504**	.319*	.499**	1	.916**	.916**	.852**	.852**
	Sig. (2-tailed)	.000	.000	.013	.000		.000	.000	.000	.000
Disregard of Customer Knowledge rules	Pearson Correlation	-.543**	-.447**	.199	.611**	.916**	1	1.000**	.870**	.828**
	Sig. (2-tailed)	.000	.000	.127	.000	.000		.000	.000	.000
Poor IT Structures	Pearson Correlation	-.543**	-.447**	.199	.611**	.916**	1.000**	1	.870**	.828**
	Sig. (2-tailed)	.000	.000	.127	.000	.000	.000		.000	.000
Poor Personnel Policies	Pearson Correlation	-.423**	-.504**	.081	.326*	.852**	.870**	.870**	1	.871**
	Sig. (2-tailed)	.001	.000	.539	.011	.000	.000	.000		.000
Low Remuneration	Pearson Correlation	-.251	-.682**	.342**	.304*	.852**	.828**	.828**	.871**	1
	Sig. (2-tailed)	.053	.000	.007	.018	.000	.000	.000	.000	

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

*. Correlation is significant at the 0.05 level (2-tailed).

4.3.11 Fraud Management

Respondents to this study agreed that CBA had been successful in fighting fraud with a mean rating of 3.84 and a mode of 3. In addition, respondents disagreed that at CBA fraud investigations were undertaken and completed with good time for decisive action (mean of 2.29 and a mode of 2). Respondents agreed that fraud prevention was engrained in the organization culture of CBA (Mean of 4.17 and a mode of 4). Further, respondents strongly agreed that fraud incidences were accorded due importance and investigation (Mean of 4.61 and mode of 5). Respondents were neutral that the organization fraud policy was well communicated (mean of 3.45 and a mode of 4). Finally, respondents agreed that CBA was up to date with emerging trends in fraud (mean of 4.12 and a mode of 4). This is as shown in Table 4.3 below.

Table 4.3: Management of Fraud in CBA

	Frequency	Mean	Mode	Std. Deviation
CBA has been successful in fighting fraud	60	3.84	3	0.241
Fraud investigations are completed in good time	60	2.29	2	0.365
Fraud prevention is engrained in Organization culture	60	4.17	4	0.187
Importance is accorded to fraud incidences	60	4.61	5	0.279
Fraud policy is well communicated	60	3.45	4	0.246
CBA is up to date with fraud trends	60	4.12	4	0.381

4.4 Types of Fraud

This section presents the data collected and analyzed in terms of types of fraud in CBA.

4.4.1 Management Fraud

Prevalence of management fraud was low in CBA bank. This is deduced from the spread of respondent's responses on occurrence of management fraud in the bank. According to 33% of the respondents, management fraud prevalence was high, 52% indicated that it was average, 10% indicated that it was low and 5% indicated that it was not existent. Due to the spread of responses it can only be deduced that occurrence of management fraud was high in the bank.

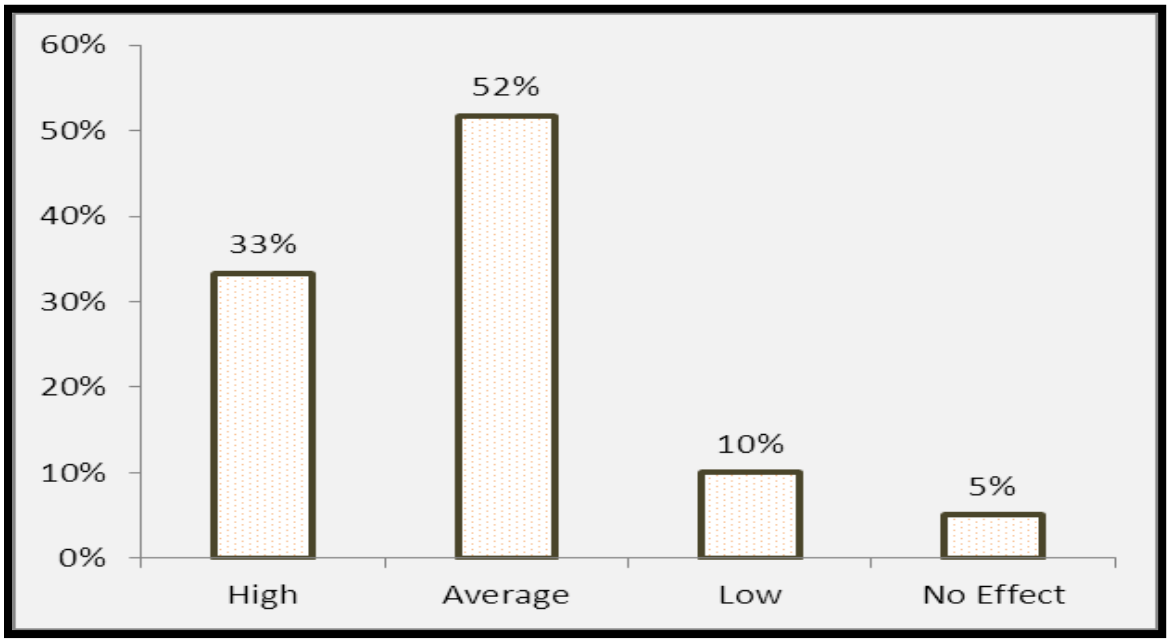

Figure 4.13: Management Fraud

Management fraud in CBA was mainly manifested in the form of overstatement of revenues with a mean rating of 2.21. This was the highest observation in the ratings on a scale of 1 – 4. Other forms of management fraud in CBA in their descending order of prevalence were:

understatement of expenses (2.37), understatement of liabilities (2.38) and overstatement of assets (2.58). This is as shown in Table 4.4 below:

Table 4.4: Forms of Management Fraud

	Frequency	Mean	Mode	Std. Deviation
Overstatement of assets	60	2.58	2	0.045
Overstatement of revenues	60	2.21	2	0.081
Understatement of liabilities	60	2.38	2	0.066
Understatement of expenses	60	2.37	2	0.059

4.4.2 Employee Fraud

Generally, employee fraud in CBA was high. Though 50% of the employees indicated that employee fraud was moderate, 40% indicated that it was high. This implies that to most employees fraud was on the higher rather than lower scales. In addition, 10% of the respondents indicated that employee fraud was low.

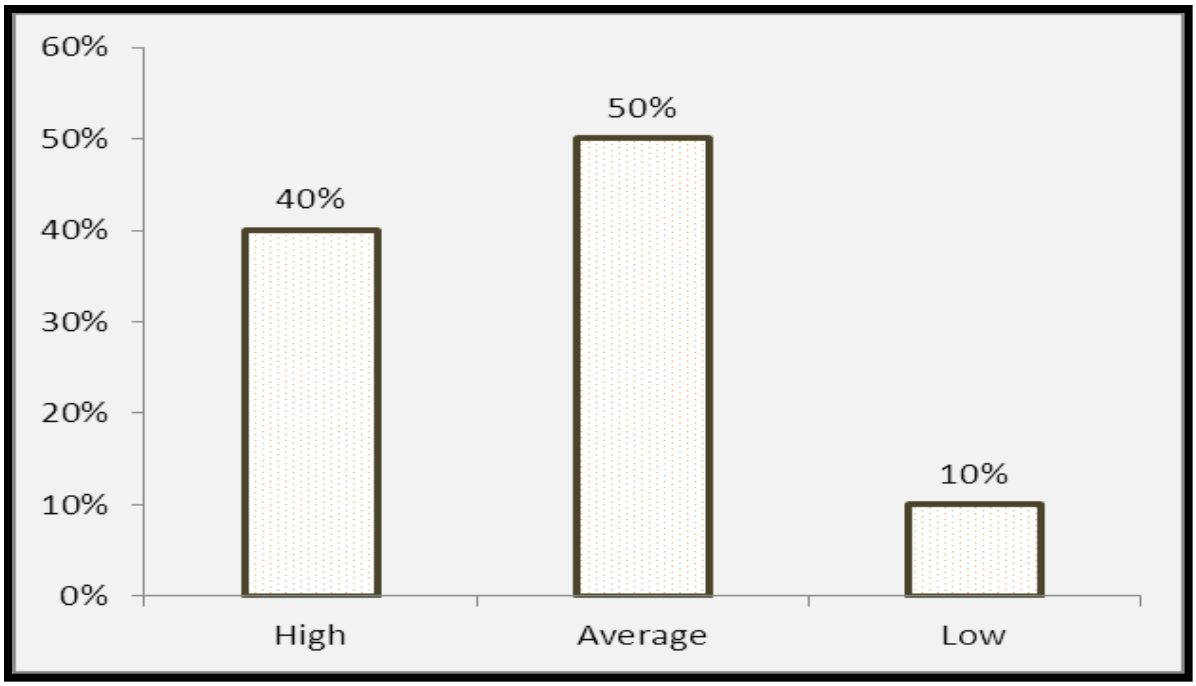

Figure 4.14: Employee Fraud

Employee fraud was mainly in the form of cash theft in the bank with a mean rating of 1.42. Other forms of employee fraud that were highly prevalent in the bank include; forgery of customers signature with a mean rating of 1.57 and computer frauds (2.15). Other forms of employee fraud present to at a lower prevalence that the above include: opening and management of fictitious accounts (2.24), use of forged cheques to withdrawal monies (2.32), diversion of funds to suspense accounts (2.41), and misappropriation of bank assets (2.57), claiming of unearned bonuses and allowances (2.74) and lending to unqualified and fictitious customers (2.89). These findings imply that the most prevalent forms of employee fraud were cash theft, forgery of customer's signature and computer frauds.

Table 4.5: Forms of Employee Fraud

	Frequency	Mean	Mode	Std. Deviation
Cash theft	60	1.42	1	0.083
Forgery of customers signature	60	1.57	1	0.047
Use of forged cheques to withdrawal monies	60	2.32	2	0.145
Opening and Operating fictitious accounts	60	2.24	2	0.067
Lending to unqualified and fictitious customers	60	2.89	3	0.145
Claiming of unearned bonuses and allowances	60	2.74	3	0.174
Diversion of funds e.g. to suspense accounts	60	2.41	3	0.274
Computer frauds	60	2.15	2	0.159
Misappropriation of banks assets	60	2.57	2	0.056

4.4.3 Employee & Outsiders

Employees and outsiders fraud was high in CBA. Thirty percent of the respondents indicated that employee and outsiders fraud was high, 57% indicated that it was average while 13% indicated that it was low. Due to the high responses by respondents indicating high prevalence, these findings imply that employee and outsider's fraud was on the higher side.

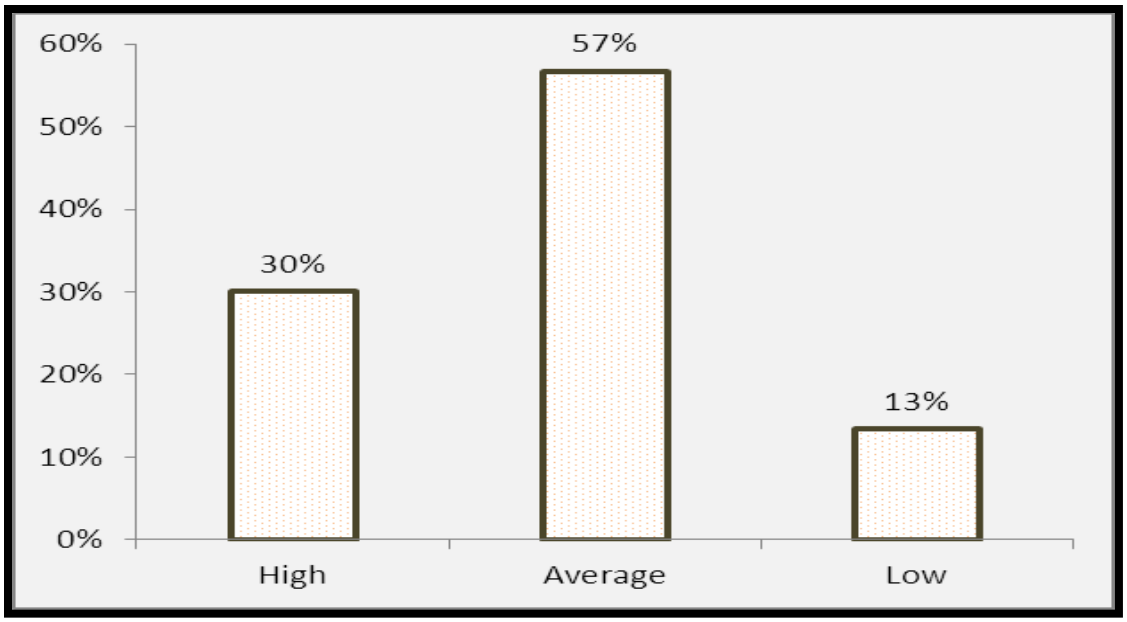

Figure 4.15: Employees and Outsiders

4.4.4 Employees & Customers

Employees and customers fraud was moderate in CBA. Evidence from data collected show that the proportion of respondents indicating an average presence of fraud was 48%, those indicating a high presence were 30% while those indicating a low presence were 22%. This implies that employees and customers fraud was moderate in the organization.

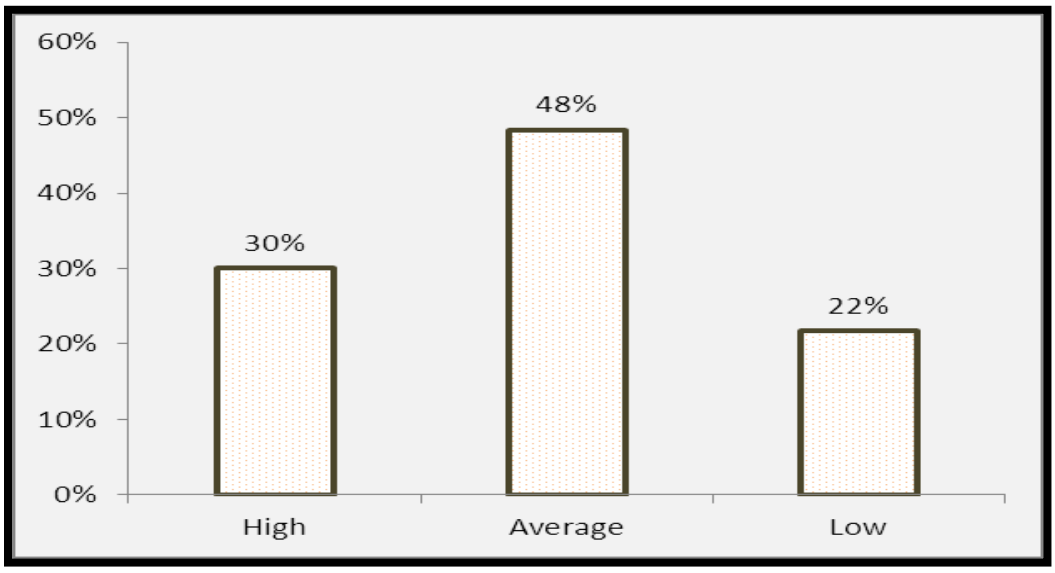

Figure 4.16: Employees and Customers

4.4.5 Employees & Management

Employees and management fraud was relatively low in CBA. According to 42% of the respondents, employees and management fraud was low, 13% indicated that it was nonexistent, 20% indicated that it was average while 25% indicated that it was high. Observations of the distribution of the findings imply that generally employees and management collusion to commit fraud is low.

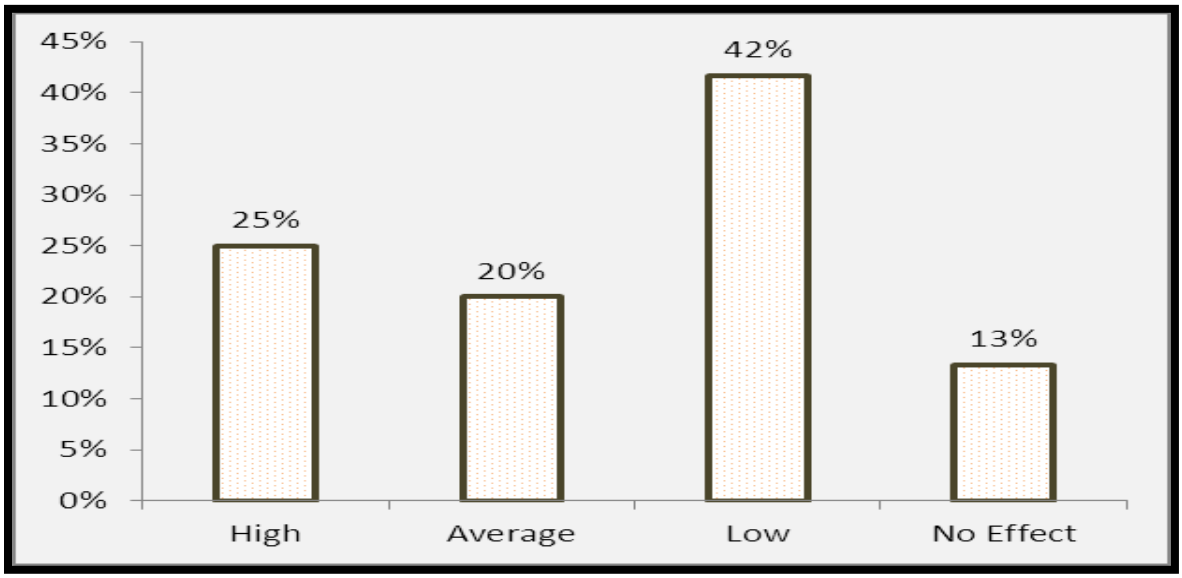

Figure 4.17: Employees & Management

4.4.6 Forms of Third Party Fraud

This study has identified the presence of employees and customers fraud, employees and management fraud and employees and third party frauds though at differing intervals and prevalence. All this can be categorized into third party frauds as they involve a third party. Forms of third party fraud identified in this study in their descending order of prevalence were: clearing frauds (transfer to wrong beneficiaries) (1.77), card fraud (2.12), misrepresentation and impersonation (2.28), letters of credit fraud (2.43), use of forged documents and counterfeits (2.45), cheque fraud (2.47) and kitting i.e. use of cheque clearing times to obtain loans (2.59). These findings are in tandem with qualitative data collected.

Table 4.6: Third Party Fraud

	Frequency	Mean	Mode	Std. Deviation
Cheque fraud	60	2.47	2	0.071
Kitting (using cheque clearance times to obtain loans)	60	2.59	2	0.062
Misrepresentation and impersonation	60	2.28	2	0.024
Use of forged documents and counterfeits	60	2.45	2	0.067
Computer/money transfer frauds	60	2.58	2	0.084
Clearing frauds (Transferring to wrong beneficiaries)	60	1.77	1	0.061
Letters of credit fraud	60	2.43	2	0.048
Card fraud	60	2.12	2	0.066

4.5 Prevention and Control of Fraud

The section presents the findings of the study on the most effective strategies for prevention and control of fraud.

4.5.1 Internal Control Systems

According to 63% of the respondents to this study, strengthening of internal controls and the accounting systems was a very effective strategy towards prevention and control of fraud. In addition, 37% of the respondents indicated that strengthening of internal controls was an effective strategy towards prevention and control of fraud.

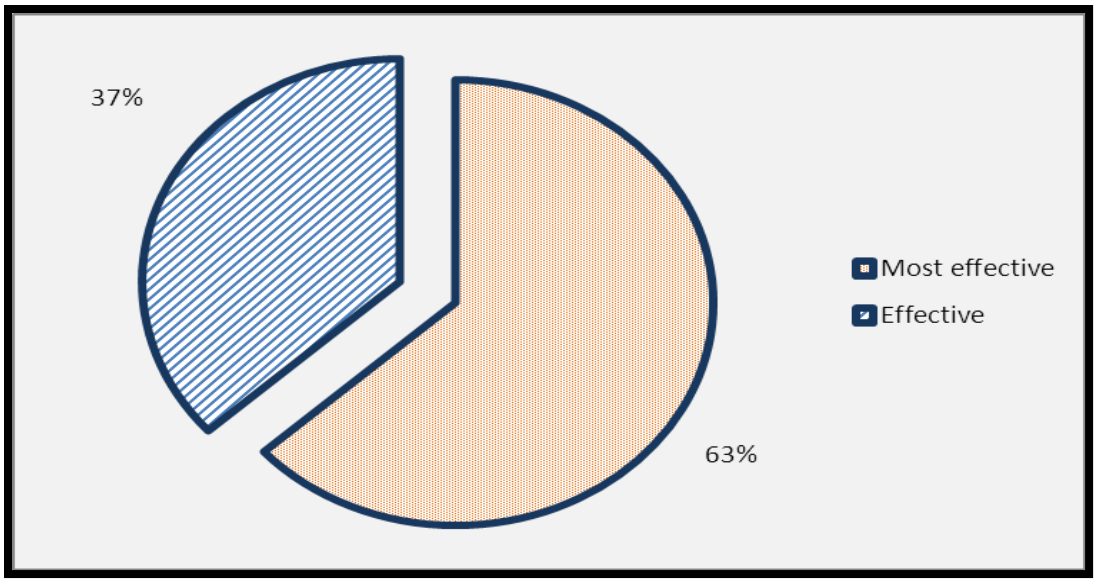

Figure 4.18: Strengthening of Internal Control Systems

4.5.2 Prosecution of Fraud Cases

Forty five percent of the respondents to this study indicated that assessment and prosecution of fraud cases was the most effective strategy towards control of fraud. Fifty two percent indicated that was effective while 3% indicated that it was least effective. This shows that to most respondents prosecution of fraud cases was effective in prevention and control of fraud.

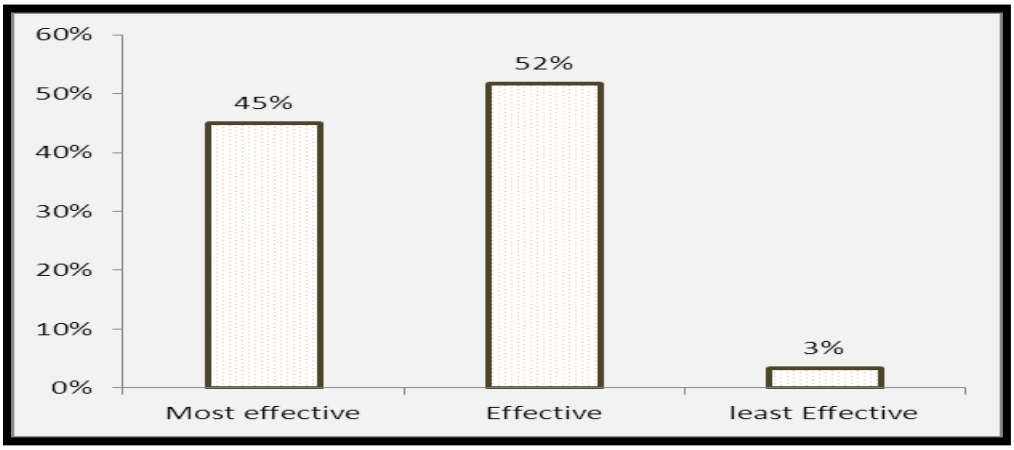

Figure 4.19: Prosecution of Fraud Cases

4.5.3 Tracking of Fraud Cases

Tracking of fraud cases was an effective strategy towards prevention and control of fraud. This is deduced from the 48% of the respondents indicating that it was the most effective while 43% indicated that it was effective. Eight percent of the respondents indicated that it was least effective. From the findings, tracking of fraud cases was a highly effective strategy towards prevention and control of fraud.

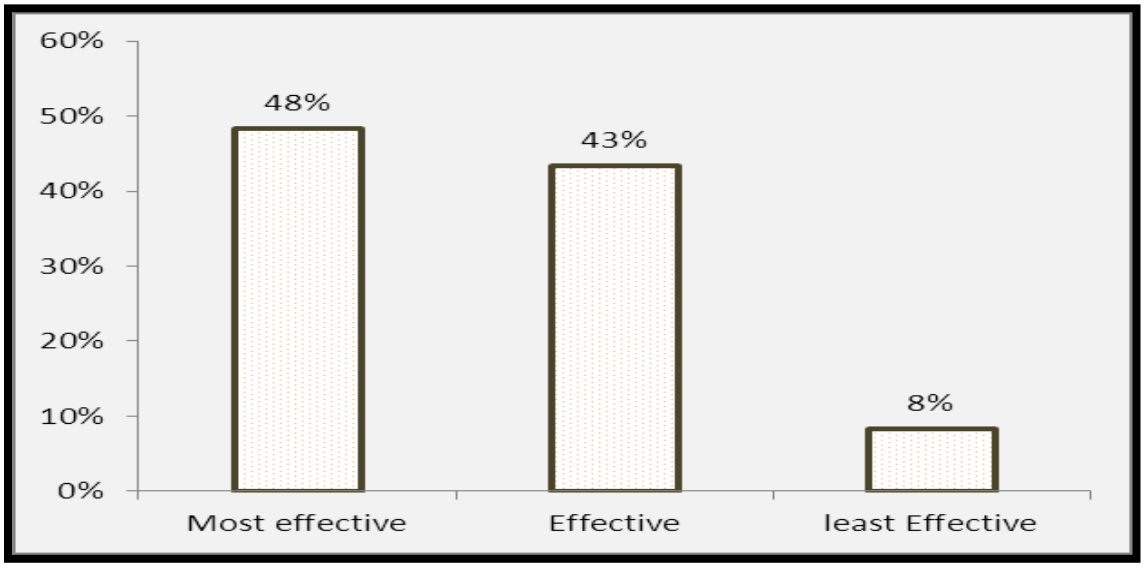

Figure 4.20: Tracking of Fraud Cases

4.5.4 Ethical Working Culture

Respondents were equally split on the effectiveness of an ethical working culture in employees in prevention and control of fraud. Fifty percent of the respondents indicated that it was effective while the remainder indicated that it was most effective. This implies that ethical working culture is effective in prevention and control of fraud.

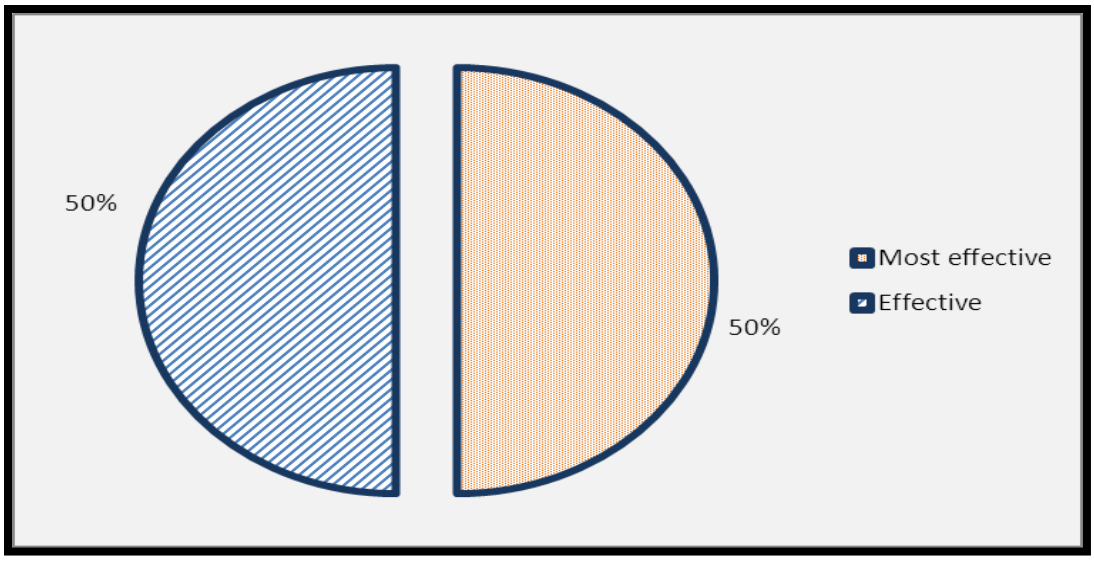

Figure 4.21: Ethical Working Culture

4.5.5 Encouragement & Incentives

Encouragement of employees through communication, rewards and recognition was a very effective strategy for prevention and control of fraud. This was according to 75% of the respondents who indicated that it was most effective and 20% who indicated that it was effective. Five percent of the respondents indicated that it was the least effective strategy.

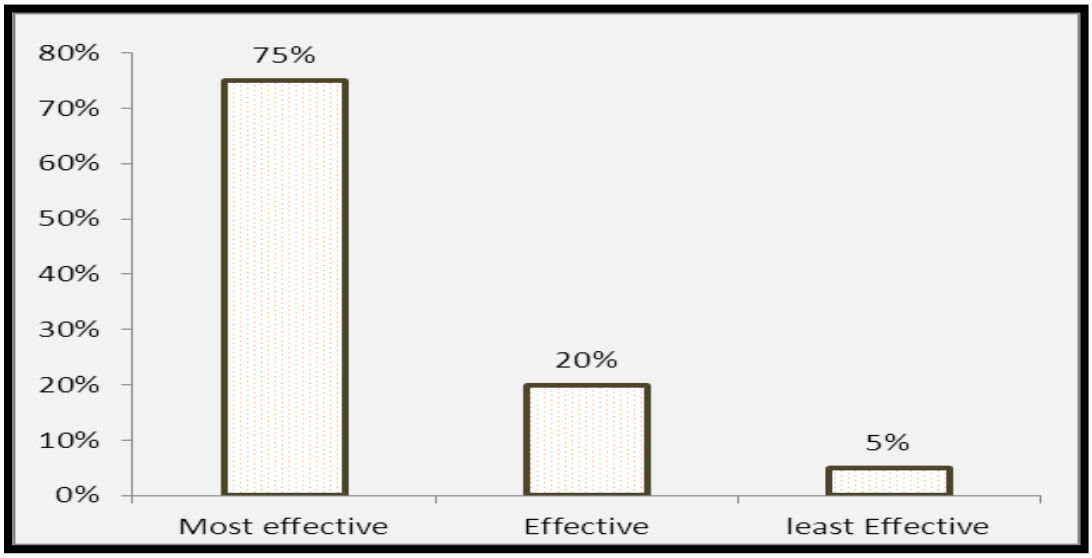

Figure 4.22: Encouragement & Incentives

4.5.6 Remuneration

Higher remuneration for employees was an effective strategy for prevention and control of fraud. This is according to 40% of the respondents who indicated that it was most effective, 42% indicated that it was effective while 18% indicated that it was least effective.

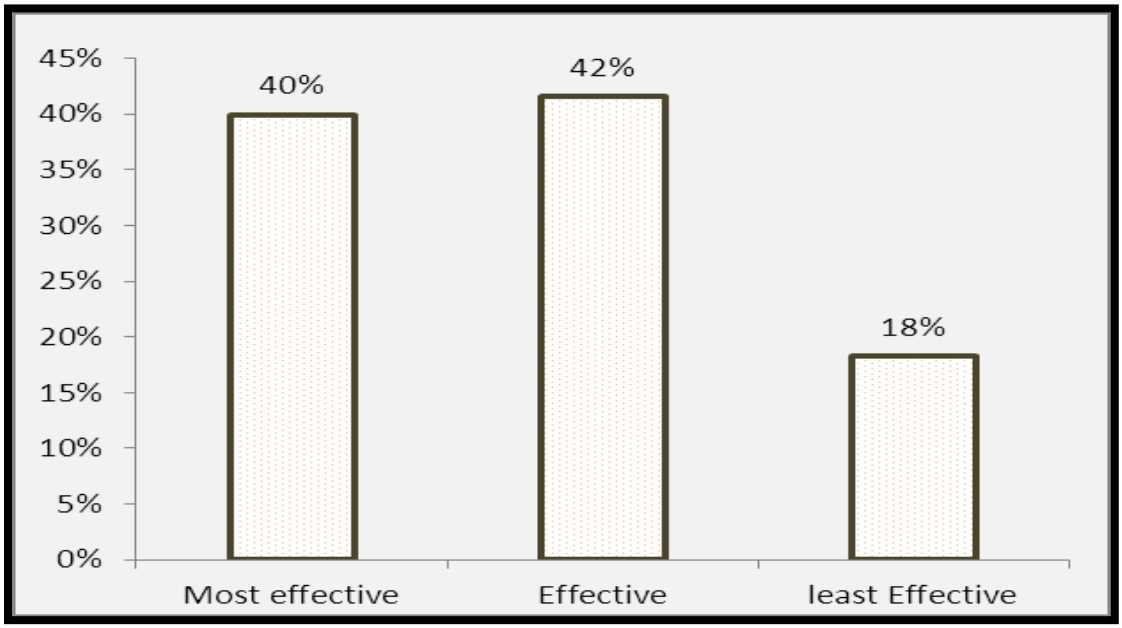

Figure 4.23: Remuneration of Employees

4.5.7 Policies

Implementation of policies to track employees conduct and background is a very effective strategy towards prevention and control of fraud. Fifty two percent of the respondents to this study indicated that it was most effective, 42% indicated that it was effective while 7% indicated that it was least effective.

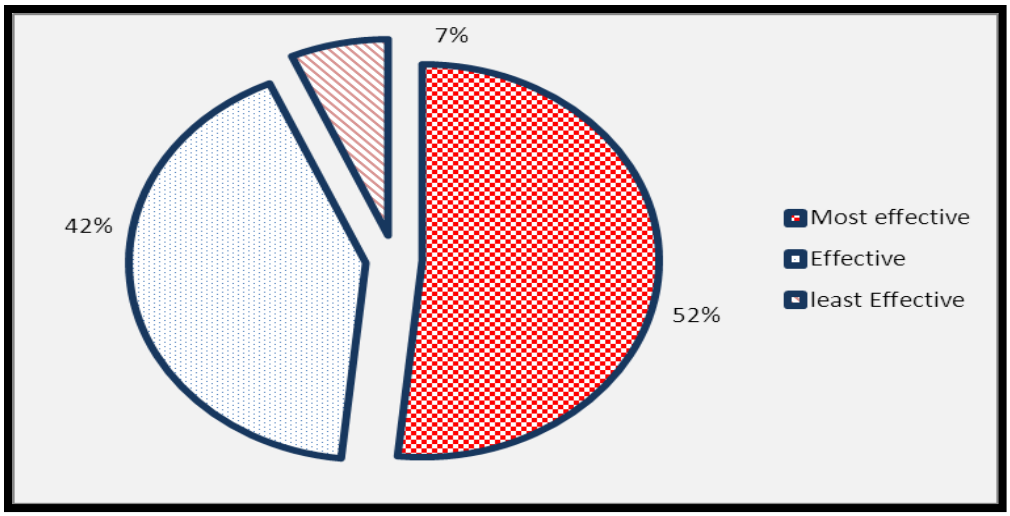

Figure 4.24: Use of Policies

4.5.8 Performance Management

The use of performance management systems, appraisals and career development incentives was a very effective strategy towards prevention and control of fraud. Seventy percent of the respondents to this study indicated that it was most effective, 24% indicated that it was effective while 6% indicated that it was not effective. Due to the high proportion of respondents indicating that it was very effective, this study concludes that use of performance management systems, appraisals and career development was a very effective strategy for prevention and control of fraud.

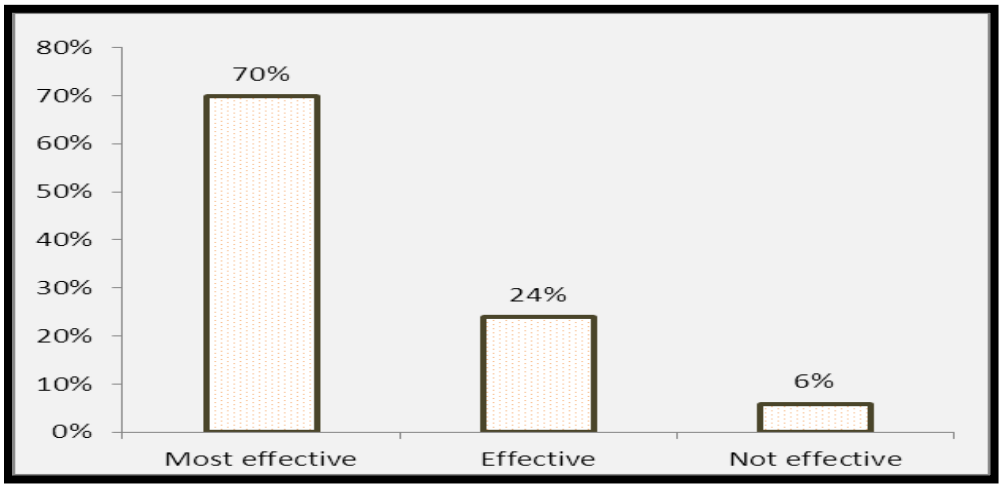

Figure 4.25: Performance Management

4.5.9 Hiring Systems and Policies

According to 53% of the respondents, adoption of well laid out hiring policies that seek the background of employees was very effective in controlling and preventing fraud. Forty two percent of the respondents indicated that it was effective while 5% indicated that it was least effective. This shows that use of proper hiring systems and policies was highly effective in controlling and preventing fraud.

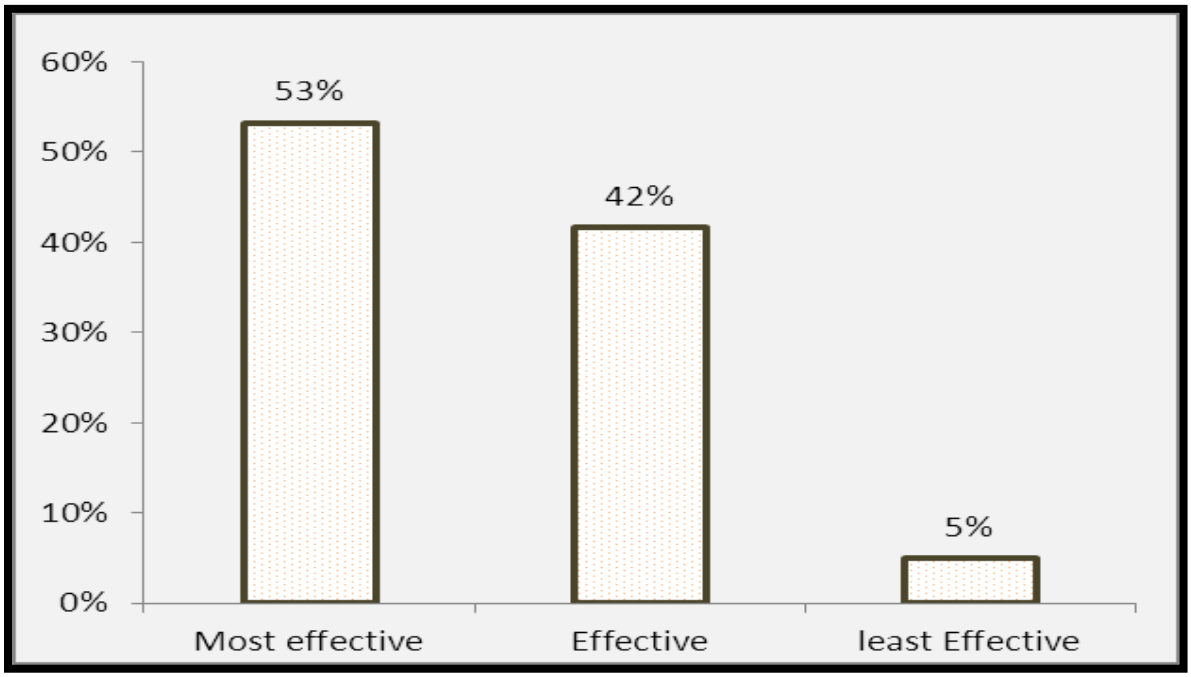

Figure 4.26: Hiring Systems and Policies

4.5.10 Audits

The use of expected and unexpected audits was very effective in controlling and preventing fraud. This is deduced from 63% of the respondents who indicated that it was very effective and 37% of the respondents who indicated that it was effective.

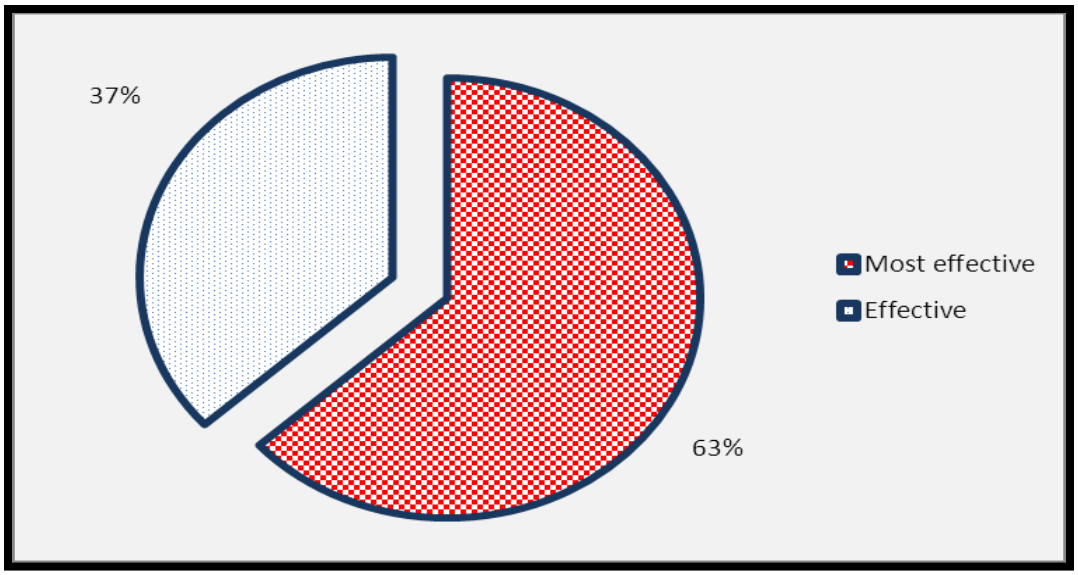

Figure 4.27: Use of Expected and Unexpected Audits

4.5.11 Employee Fraud Schemes and Policy

Employee fraud schemes and policies were most effective in controlling and preventing fraud. This is according to 52% of the respondents who indicated that it was most effective. Thirty seven percent of the respondents indicated that it was effective while 12% indicated that it was least effective.

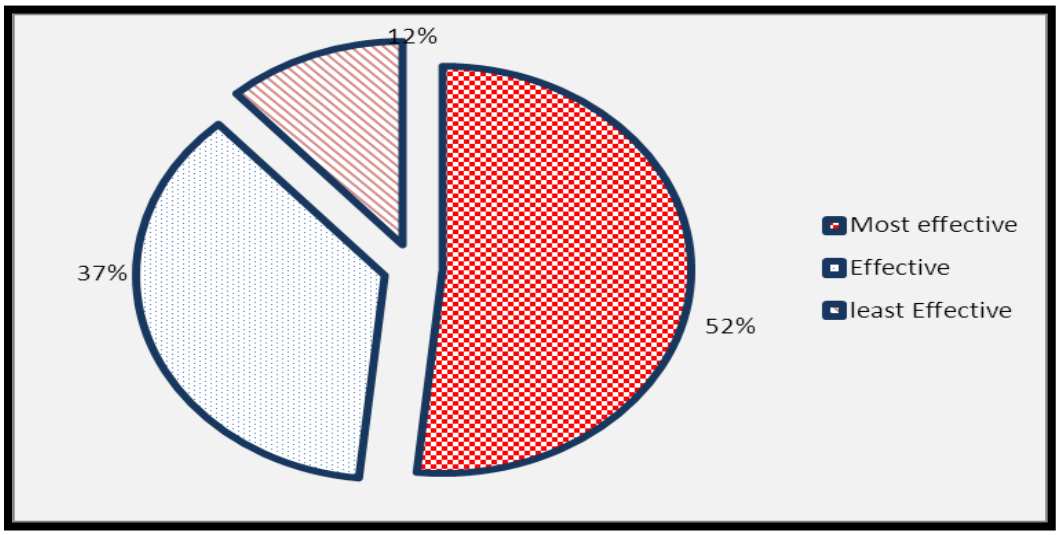

Figure 4.28: Employee Fraud Schemes

4.5.11 Use of Hotlines

Furthermore this study found that the use of fraud reporting centers and hotlines was effective in controlling and preventing fraud. Forty seven percent of the respondents indicated that it was most effective, 52% indicated that it was effective and 2% indicated that it was not effective.

Table 4.2: Fraud Reporting Centers and Hotlines

	Frequency	**Percent**
Most effective	28	47
Effective	31	52
Not effective	1	2
Total	**60**	**100**

4.5.12 Employee Vacation

Shuffling and mandatory vacations for employees was an effective strategy for the control and prevention of fraud. This is according to 43% of the respondents. A similar proportion indicated that shuffling and mandatory vacations for employees was the most effective strategy while 13% of the respondents indicated that it was the least effective strategy.

Table 4.3: Shuffling and Mandatory Vacations

	Frequency	**Percent**
Most effective	26	43
Effective	26	43
Least effective	8	13
Total	**60**	**100**

4.5.13 Use of ICT

The use of ICT tools such as passwords and firewalls was the most effective strategy for prevention and control and fraud. This is due to the high proportion of respondents (82%) who indicated that it was the most effective. Eighteen percent of the respondents indicated that it was effective.

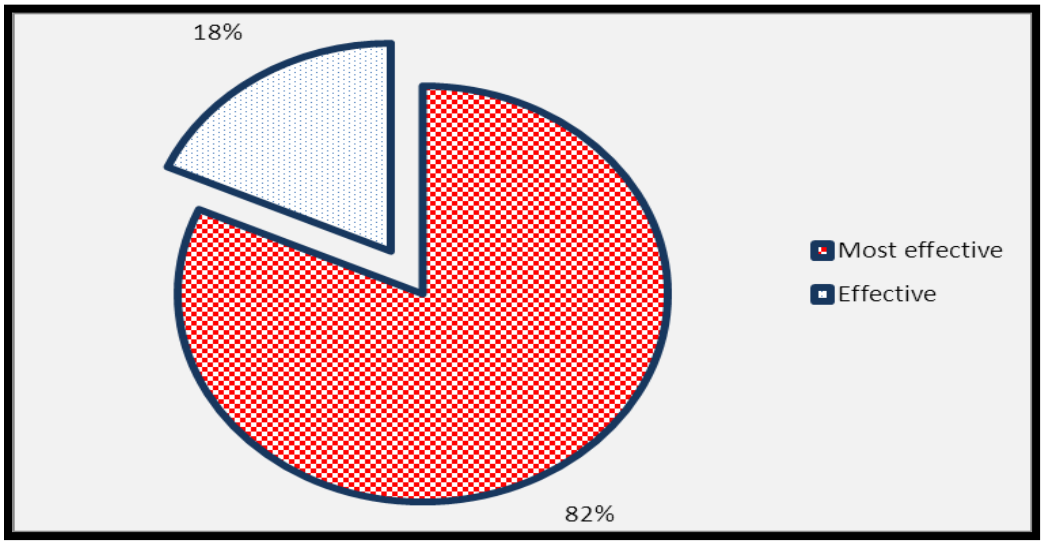

Figure 4.29: Use of ICT Tools

4.5.14 Use of Analytical Tools

According to 60% of the respondents, the use of analytical tools to detect and prevent fraud was very effective in controlling and preventing fraud. Twenty percent indicated that it was effective while a similar proportion indicated that it was least effective.

This implies that the use of analytical tools to detect and prevent fraud was very effective in controlling and preventing fraud.

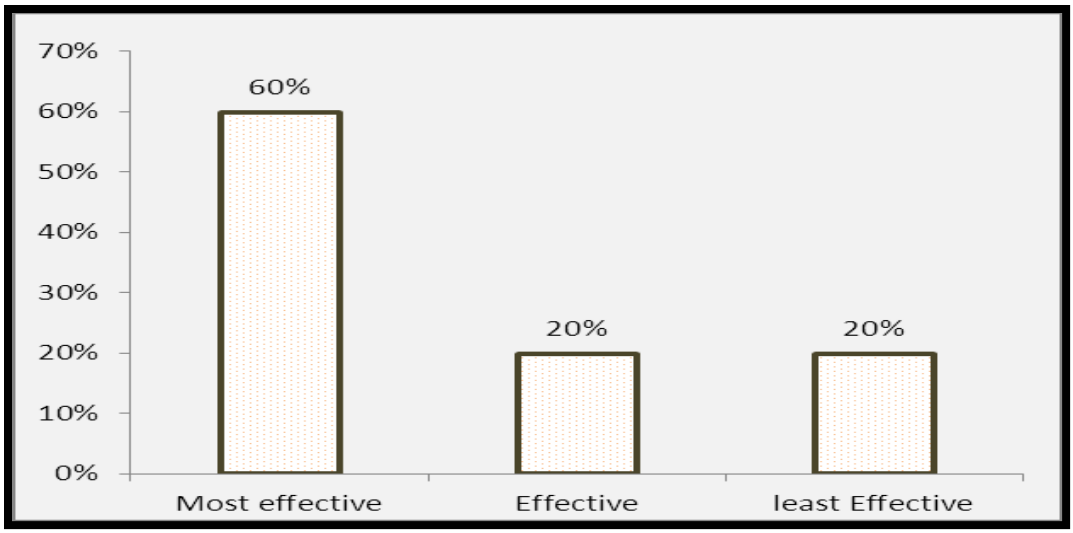

Figure 4.30: Use of Analytical Tools

4.5.15 Other Strategies

Respondents indicated other strategies that could be used to prevent and control fraud in the Bank. Some of the strategies identified include: upgrading the ATM cards used from magnetic strips to chip and enhancing pins, educating customers on card safety, proper procurement and disposal systems, open door policies for employees, staff training and treatment of fraud cases by employees equally.

4.6 Chapter Summary

This chapter has presented the findings and results of the study. The study used majority of its respondents from fraud auditors and supervisors who had the primary responsibility of detecting and preventing fraud. This enhances the findings of the study. The study found that fraud in CBA was accorded very high priority. The major causes of fraud in the bank were availability of opportunities for fraud, rationalization of fraud acts and pressure to commit fraud.

Secondly, this study found that employee fraud was the most common fraud in the bank while third party fraud was second. Management fraud in CBA was very low. Some of the

forms of fraud identified include: cash theft, use of forged documents, cards fraud, letters of credit fraud and impersonation.

Finally, this study found that there are very effective strategies to prevent and control fraud. However, the most effective strategies for prevention and control of fraud are: use of ICT tools such as passwords and firewalls, strengthening of internal controls and systems, encouragement, communication, rewards and recognition of employees, performance management, improvement and hiring systems and policies, use of expected and unexpected audits and use of analytical tools. The findings as presented in this chapter are discussed, summarized and concluded in Chapter five. In addition, the chapter presents recommendations for practice as well as those for further studies.

CHAPTER FIVE

5.0 DISCUSSION, CONCLUSIONS & RECOMMENDATIONS

5.1 Introduction

Chapter five discusses the findings and results presented in Chapter four. Discussion is in view of the findings of this study and those of other scholars and researchers. In addition, this chapter presents conclusions and recommendations for the study.

5.2 Summary

This study sought to assess fraud in the banking industry in Kenya using Commercial Bank of Africa as the case. The objectives of the study were: to establish the causes of fraud at Commercial Bank of Africa, examine the types of frauds committed and determine the appropriate strategies for prevention and control of fraud.

The study utilized a descriptive research design using CBA bank as the case. The study was conducted during the months of February and March 2014 using all employees of CBA with Nairobi County. In total 68 employees representing 33% of the populations were included in the sample size using a stratified random sampling technique. Data for the study was collected using an online questionnaire for cost and convenience to all the respondents. However, the questionnaire was pretested for errors and relevance. Data collected was analyzed using SPSS vs. 20 for means, frequency distributions, standard deviations and modes. Analyzed data was presented using figures and tables for ease of interpretation and elaboration.

The study found that fraud in CBA was accorded very high priority. The major causes of fraud in the bank were availability of opportunities for fraud, rationalization of fraud acts and pressure to commit fraud. Opportunities for fraud were present due to relaxed internal controls and accounting systems, inadequate supervision of subordinates, disregard for customer due diligence requirements and poor personnel policies.

Secondly, this study found that employee fraud was the most common fraud in the bank while third party fraud was second. Management fraud in CBA was very low. Some of the forms of fraud identified include: cash theft, use of forged documents, cards fraud, letters of credit fraud and impersonation.

Further, this study found that there are very effective strategies to prevent and control fraud. However, the most effective strategies for prevention and control of fraud are: use of ICT tools such as passwords and firewalls, strengthening of internal controls and systems, encouragement, communication, rewards and recognition of employees, performance management, improvement and hiring systems and policies, use of expected and unexpected audits and use of analytical tools.

5.3 Discussion

This section discusses the findings and results of the study in light of existing evidence and literature from other researchers.

5.3.1 Factors Contributing to Fraud

Fraud is accorded high priority in CBA. The management of CBA takes great initiative to detect, punish and control cases of fraud in the bank due to its negative impact on credibility and performance of the bank. However, the primary responsibility of controlling and preventing fraud in CBA lies with the fraud analyst and auditors.

Though very many causes of fraud exist in the CBA, the availability of opportunities for fraud was the most dominant factor. This study found that the most common cause of fraud in CBA was opportunity to commit fraud. Other factors identified include: rationalization of the act of fraud and pressure to commit fraud. Wilson (2004), Hillison *et al*. (1999) and CIMA (2009) had similar findings in their study when they noted that, opportunity is the first and important element in fraud .This is the part of the equation that an organization can effectively use to deter employee dishonesty through policies, procedures and processed.

In addition, the international accounting organization CIMA (2009) noted that some of the factors leading to fraud in banks include: rationalizing their prospective crimes away, opportunities to commit crimes, perceived suitability of targets for fraud, technical ability of the fraudster, expected and actual risk of discovery after the fraud has been carried out, expectations and consequences (job loss, family stigma and proceeds of crime confiscation and actual consequences of discovery. However, only some of the factors identified by CIMA were identified in this study. This is because, while the study by CIMA was worldwide, this study was based on one single Kenyan banking institution.

The study sought to identify the specific factors that led to fraud in CBA. The specific factors with a high causative effect on fraud in CBA were: weak internal control and accounting systems, inadequate supervision of subordinates, disregard for customer knowledge rules and poor IT structures. Of these factors, weak internal control and accounting systems was identified by most respondents as the most driving factor for fraud. Other factors that contributed to fraud though in a less extent were: poor personnel policies and low remuneration of employees.

These findings are similar to the findings of Kingsley (2012) in his study on banking fraud in Nigeria. In the study, Kingsley (2012), Wang and Klenier, (2005) and ACFE (2009) found that institutional factors that lead to fraud may include but are not limited to weak accounting system control systems, inadequate supervision of subordinates, disregarding for Know Your Customer rule, poor information technology and data base management, hapless personnel policies, poor salaries and general frustration occasioned by management unfulfilled promises. Other factors identified by Kingsley (2012), ACFE (2009), Cressey (1973) include, failure to engage in regular call over, employees refusal to abide with laid down procedures without any penalty, banks reluctant to report fraud due to the perceived negative publicity, banking experience of staff and inadequate infrastructure that may include poor communication systems result to a buildup of unbalanced posting, inadequate training, poor book keeping and genetic traits like kleptomaniac who pathologically steals for fund.

This study identified some of the factors while others were not identified due to various reasons e.g. they were not identified by this study while some were not included in the data collection instrument.

This study sought to investigate how and the extent to which CBA manages fraud in the organization. The study found that the CBA has been very successful in fighting fraud. In addition, the study found that fraud prevention is engrained in the organization culture, importance is accorded to fraud incidences and CBA is up to date with current and emerging fraud trends in the environment. However, the study found that fraud investigations were not undertaken and completed in good time.

5.3.2 Types of Fraud

There are various types of frauds occurring in CBA. While some of the frauds are at the managerial level, others occur due to insider collusion between employees while others occur as a result of collusion between employees and outsiders/third parties.

Nevertheless, this study found that the most common types of fraud in CBA are: employee (insider frauds). Others occurring in the bank in their descending order of frequency includes: employees and outsiders, employees and management and management level fraud. Though other scholars did not rate the occurrence of the types of fraud, they had similar findings or observations to those of this study.

Employee fraud which was the most common occurred in the form of: forgery of customers signatures, computer frauds, opening and management of fictitious accounts, use of forged cheque to withdrawal monies, diversion of funds to suspense accounts, misappropriation of bank assets, claiming of unearned bonuses and allowances and lending to unqualified and fictitious customers. However, customer's signatures and computer frauds were the most common types of employee fraud.

Employee fraud also known as non-management fraud and is usually perpetrated by the employees of the banks (Kingsley, 2012). The main causes of employee fraud are as listed above and supported by the findings of Kingsley (2012), Cressey (1973), and ACFE (2009).

Management fraud which was the least common was manifested in the form of overstatement of revenues. Other managerial level frauds occurring though at a reduced frequency include: understatement of expenses, understatement of liabilities and overstatement of assets. However, these cases of management fraud were very rarely identified. This could be attributed to stringent reporting rules and regulations imposed on the bank by the Central Bank of Kenya and the International Financial Reporting and Accounting regulations. These findings are in line with the findings of Kingsley (2012), who noted that management fraud is aimed at painting the bank in good light to the investors, creditors and regulatory authorities. Though management fraud manifests though overstatement of assets or revenues and understatement of liabilities and expenses, the Association of Certified Fraud Examiners believes that it is carried out through fictitious revenues, timing difference, improper asset valuation concealed liabilities and expenses and improper or inadequate discourse (Kingsley, 2012).

Third party frauds were inherent in CBA though at low rates. According to this study, third party frauds occurred in the form of employees and outsiders, employees and customers and employees and management. The low observation of employees and management fraud could be attributed to the organization structure design and reporting stations which are independent. Furthermore, rigorous auditing and risk management structures and systems could reduce the occurrence of management and employees fraud.

Nevertheless, when third party fraud occurred it was mainly in the form of clearing frauds (transfer to wrong beneficiaries), card fraud, misrepresentation and impersonation, use of forged documents and counterfeits, cheque fraud, and kitting i.e. use of cheque clearing times to obtain loans. These factors are presented in their descending order of frequency. Similar findings were presented by Onkagba (1993) who identified cheque fraud, forgeries

(Akinyomi, 2012), kitting, misrepresentation and impersonation, counterfeit securities, money transfer fraud, clearing fraud and letter of credit fraud (Onkogba, 1993: Adeoti, 2011; Akinyomi, 2012; Zhang, 2013)

5.3.3 Prevention and Control of Fraud

There are various structures and systems embedded in CBA management and organization structure to detect, prevent and control fraud. While some of the strategies are internal others are external in nature. This study however, focuses on the internal strategies employed to prevent and control fraud.

According to this study the strategies employed to control and prevent fraud include: strengthening of the internal control systems and accounting structures, identification, investigation and prosecution of fraud cases, tracking of fraud cases, introducing and cultivating an ethical working culture for employees and the use of encouragement, incentives, rewards and recognition. Other effective strategies for prevention and control of fraud include: implementing fraud management policies, use of performance management and appraisal systems, undertaking hiring systems and policies that undertake due diligence on employees, undertaking unexpected and expected audits and implementing employee fraud schemes e.g. reporting centers and hotlines, shuffling and mandatory vacations for employees. Use of ICT tools such as passwords and firewalls, and the use of analytical tools were also effective tools for management and control of fraud. However, use of remuneration of employees was not an effective tool for preventing and controlling fraud.

Similarly, Gates and Jacob (2009) noted that fraud risk needs to be assessed for each are and process of the business for example cash payments, cash receipts, sales, fixed assets and loans. Given the prevalence of fraud and the negative consequences associated with it, there is compelling evidence and arguments that organizations should invest time and resources towards tracking fraud. Based on causes of fraud, we see the most effective ways to deal with fraud issue is to adopt methods that will decrease motive, restrict opportunity, and limit the ability for potential fraudsters to rationalize their actions (CIMA, 2009).

Kingsely (2012); Douglass and Malthus, (2009) similarly noted that to guarantee effective strategies of fraud prevention and control, banks are to ensure that operational systems are designed with inbuilt control devices. Banks can reduce or better still eradicate frauds and forgeries if all control devices built into the system are respected. Some of the effective strategies identified include: An encouraging working atmosphere makes employees follow established policies and procedures and operate in the best interest of the organization; an ethical culture includes defining principles and values that reflect a desire for high ethical standards and a no tolerance position on fraud. Furthermore, companies should ensure they conduct a background check that covers criminal history, education, previous employment, civil history for possible lawsuits before employing anyone, unannounced financial audits and fraud assessments, sound internal control, implementing a fraud policy, a confidential 24/7 hotline, anonymous tips, mandatory vacation policy, use of risk management information system, use of analytical views and proper password use (Bierstake *et al.,* 2006; Hillison *et al*, 1999; ACFE, 2009; CIMA, 2009; Kingsley 2012; Douglass & Malthus, 2009; Gates & Jacob, 2009).

While all the above strategies were identified as effective, some of the factors were identified as most effective. This study identified the use of ICT tools such as passwords and firewalls, use of analytical tools, employee fraud schemes and policy, use of expected and unexpected audits, proper hiring systems and policies, performance management and strengthening of internal control systems as the most effective tools for prevention and control of fraud. This could be the reason for system upgrades include the core banking system and the card management systems undertaken by the bank during the course of the study.

5.4 Conclusions

Based on the findings and discussion of the findings of this study, the following conclusions were made.

5.4.1 Factors Contributing to Fraud

This study concludes that the most dominant factor influencing or accelerating fraud in CBA was the availability of opportunities for fraud. These opportunities were presented as a result of weak internal control and accounting systems, inadequate supervision of subordinates, disregard for basic customer and employee management structures.

Secondly this study concludes that establishment of an ethical culture in within the organization structure and environment, research and knowledge of fraud trends and constant review, measurement and control of fraud and fraud systems in the bank are critical for management of fraud.

5.4.2 Types of Fraud

This study concludes that employee fraud is the most common form of fraud in CBA. Employees are the primary drivers of fraud through forging of documents, opening and management of fictitious accounts, claiming unearned benefits and computer frauds.

On the other hand, this study concludes that financial reporting rules and regulations in addition to regulatory information provision rules by Central Bank of Kenya (CBK) have been effective in containing management fraud. This is because management fraud in CBA was very rare.

5.4.3 Prevention and Control of Fraud

Banks must undertake all measures to prevent and control fraud. Though various strategies are effective in preventing and controlling fraud, this study concludes that the most effective strategies are: use of audits, deployment of ICT security measures such as passwords and firewalls, use of analytical tools, strengthening of internal controls and accounting systems and use of human resource management systems.

5.5 Recommendations

The following recommendations are made:

5.5.1 Recommendations for Practice

These recommendations are for policy making at the organization/ industry level. Furthermore, these recommendations can be utilized at the practice or management level.

5.5.1.1 Factors contributing to fraud

As per the findings of this study, fraud in banks is driven by the availability of opportunities. Therefore, this study recommends that banks should implement systems and structures that reduce the opportunities for fraud. In addition to strengthening internal control systems and structures, banks can use ICT tools to reduce opportunities or instill punitive measures for employees engaging in fraud and fraud related incidences.

In addition, this study recommends that banks should strictly adhere to due diligence rules and regulations imposed by the CBK on customers and employees. This will allow banks to have background knowledge on employees and customers. Where regulations on due diligence are not available, banks should develop custom made bank specific rules and regulations. In addition, these rules must be applied without exemption. This study further recommends that banks should engrain in their organizational culture: ethical practices in employees.

5.5.1.2 Types of Fraud

Employee related frauds are the most common in banks. This is through the use of forged documents, card fraud, computer fraud and diversion of funds to suspense accounts, misappropriation of assets and claiming of unearned benefits. This study recommends that banks should decentralize the multiple functions of employees i.e. employees dealing with authentication of customers signatures do not have access to account details such as balance.

Furthermore, employees must be rotated on regular basis to reduce cases of familiarity in one specific area.

To reduce third party frauds, banks should instill multiple authentication of transactions i.e. managers approve transactions of accounts that are dormant or high value customers. This could reduce the cases of fraud especially with the findings that management and employee frauds are very low. In fact, banks must use these findings to their advantage by requiring managerial level supervision and authentication of certain transactions i.e. acquiring of loans on postdated cheque/kitting, review or change of details in cards.

However, it is expected that with the introduction of electronic cheque clearing systems and the introduction of EMV chipped cards and Pins, some of the cases of third party fraud will dramatically reduce.

5.5.1.3 Prevention and Control of Fraud

To reduce the cases of fraud in banks, this study recommends that ICT should be utilized as it is easy to track, easy to use and useful. The use of ICT will enhance accountability and transparency of employees as access to the system is tracked and recorded. Therefore cases of fraud are easily identified and culprits prosecuted. Indeed, ICT could be the cure to fraud in the banking industry. This could inform the rush by most banks to upgrade their core banking systems and card management systems.

In addition, this study recommends the strengthening of internal controls and accounting systems, the use of analytical tools to analyze and present statistics on fraud, use of audits and employee fraud schemes to combat fraud. Specifically, every bank must have fraud management units where all fraud related incidences are investigated and reported.

5.5.2 Recommendations for Future Studies

To validate the findings of this study, this study recommends that future studies be replicated in different banks or financial institutions. This could be undertaken in a large bank

especially the top 5 banks in asset size in Kenya or the East African region. Furthermore, a similar study using multiple banks could also provide substantive literature for comparison. This could provide literature for comparison to the findings of this study.

Secondly, this study recommends research on the impact of fraud on bank performance. Though it is generally perceived to be negative, the magnitude or extent of the impact has not been examined and this could provide literature on how fraud affects various performance indicators of the bank.

Finally, this study recommends a research on the impact of fraud management policies on bank performance. The Central Bank of Kenya, Kenya Bankers Association and the International Financial Reporting Standards all impose regulations on the type, form and frequency of reporting of banks. This has led to the reduction of management fraud. Could this have a positive effect on bank performance? Furthermore, have the introduction of this policies led to the reduction of other forms of fraud? These are the questions the study should seek to answer.

REFERENCES

Abdul R., Babaitu, D., & Tinusa, G. (2012). Fraud and its implications for bank performance in Nigeria. *International Journal of Asian Social Science,* vol. 2 no. 4 pp. 35-45.

Adeniji, A. (2004). Auditing and investigation. Landmark Publisher: Lagos

Adewumi, S. (2011). *An Ideal ATM Implementation in an Unsecured Environment.* University of Jos Press.

Akindele, R. I. (2012). Fraud as a negative catalyst in the Nigerian banking industry. *Journal of Emerging Trends in Economics and management Sciences* (JETEMS) Vol. 1 pp. 44 -56

Akinyomi, O. J. (2012). Examination of fraud in the Nigerian banking sector and its prevention. Asian Journal of Management Research, 3(1), 182-194.

Albrecht, W.S. (1996). Employee fraud. *Internal Auditor,* October, p. 26.

Association of Certified Fraud examiners (ACFE), (2008).*Report to the Nation on Occupational Fraud and Abuse,* www.acfe.org

Berger, H.S. & Gearin ,W.F. (2004). Due diligence: two important words for all those who wear the white hats. *RMA Journal,* Oct.

Bierstaker, J. Brody, R.G. & Pacini, C. (2006). Accountant's perception regarding fraud detection and prevention methods. *Managerial Auditing Journal,* Vol. 21, No. 5, pp 520-535.

Bologna, J. (1993) *Handbook on Corporate Fraud*, Butterworth-Heinemann, Stoneham, MA, pp. 54-62.

Central Bank of Kenya (2013). Financial Institutions in Kenya. www.cbk.go.ke

Chartered Institute of Management Accountants (CIMA) (2009). Fraud Risk Management: A guide to good Practice. CIMA.

Clark, J. P. &Hollinger, R. C., (1983). Theft by employees. Lexington, MA: LexingtonBooks.

Commercial Angles Newsletter. (2001). Fraud Prevention. July, available at www.commercialangles.com/articles/fraud_control.html.

Commercial Bank of Africa (2013). Employee Statistics. Payroll. Human Resource Management Department

Cooper, D. R., & Schindler, P. S. (2003). *Business Research Methods.* New York: McGraw Hill.

Cressey D. (1973). *Others Peoples Money: A study in the Social Psychology of Embezzlement.* Montclair, N. J. Patterson Smith

Criminal Investigation Department (CID) (2013). Report of investigated and prosecuted Bank related Cases in Kenya. Government of Kenya

Ganesh, A. &Raghurama, A. (2008). Status of training evaluation in commercial bank- a case Study. *Journal of Social Sciences and Management Sciences*, Vol. 37, No.2, Sept, pp 137-58.

Gates T. & Jacob K. (2009). Payment Fraud: Perception Versus Reality – A conference Summary. *Economic Perspectives* , Vol. 32 No. 1

Haugen, S. & Selin J.R. (1999). Identifying and controlling computer crime and employee fraud. *Journal: Industrial Management & Data Systems,* Vol. 99 No. 8, pp. 340-4.

Hillison, W., Pacini, C. & David S., (1999). The internal auditor as fraud-buster. *Managerial Auditing Journal*, Vol. 14 Iss: 7, pp.351 – 363

Idowu, A. (2009). An assessment of fraud and its management in Nigeria commercial banks. *European Journal of Social Sciences*, vol. 10 no. 4.

Iyiegbuniwe, W. (1998). Fraud Risk in Nigerian Banks. *Unilag Journal of Business*, vol. 1 no. 2.

Jeffords, R., Marchant, M.L. & Bridendall, P.H. (1992). How useful are the tread way risk factors? *Internal Auditor*, June, p. 60.

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.

Kothari, C.R., (1985). *Research Methodology- Methods and Techniques,* New Delhi, Wiley Eastern Limited.

Mitra, N.L. (2001). The report of expert committee on legal aspects of bank frauds.

Mohammed B. Hemraj, (2004) "Preventing corporate scandals", Journal of Financial Crime, Vol. 11 Iss: 3, pp.268 - 276

Mugenda, M. O., & Mugenda, A. G. (2003). Research Methods in Education: Quantitative and Qualitative Approach, Nairobi.

National bank of Chicago: *Fraud prevention series*. Benson and Edwards fraud prevention series (Volumes 1-11). B & E publishers Lagos.

NDIC. (2011). Annual Report and statement of Account.

Onkagba, J.O. (1993). Auditing Computerization Information System: A Growing Audit Challenge. *The Nigerian Accountant*, Lagos, Published by ICA|N, Jan/Mar

Orodho, J. (2008). *Techniques of Writing Research Proposals and Reports in Education and Social Sciences*. Nairobi: Kanezja Enterprises.

Pan, G., Seow, P. S., Suwardy, T., & Gay, E. (2011). Fraud: A review and research agenda. Journal of Accountancy Business and the Public Interest, 10, 138-178.

Pricewaterhousecoopers PWC (2009). Fraud Solutions for Africa Banks-A Kenyan Perspective. PWC, 2009.

Pricewaterhousecoopers PWC (2011). Fighting fraud in financial services. 6th PwC Global Economic Crime Survey.

Sharma, B.R. (2003). *Bank Frauds- Prevention & Detection*. Universal law Publishing Co. Pvt .Ltd.

Sharma, S. and Brahma (2000) A Role of Insider in banking Fraud. Available at http;// manuputra.com

Tchankova, L. (2002). Risk identification–basic stage in risk management. Environmental Management and Health, 13(3), 290-297.

Wang, Y., & Kleiner, B. H. (2005). Defining employee dishonesty. Management Research News, 28(2/3), 11-22.

Wels F. (2004). *Corporate Fraud Handbook – Prevention and Detection.* Wiley Hard Cover

Willson, R. (2006).Understanding the offender/environment dynamics for computer crimes. *Information Technology and people* Vol, 19, No.2, pp170-186.

Wilson D. (2004). Fraud and technology crimes findings from 2003/2004. The National Archives.UK.

Yin, R. (2003). *Case study research: Design and methods* (3rd ed.). Thousand Oaks, CA: SAGE Publications.

APPENDICES

APPENDIX I: QUESTIONNAIRE

Dear Respondent,

Please follow the link below to fill in a questionnaire that seeks your opinion of fraud in Commercial Bank of Africa Ltd. This research is being carried out in partial fulfillment of the requirement for the Degree of Masters in Business Administration (MBA).The information will assist the CBA management to understand the causes of fraud in the banking industry and best strategies to prevent it. Any information provided will be treated with utmost confidentiality and no single responses will be reported on its own but as a summation of all the responses. You will require an estimated time of about 5-8minutes to fill in the questionnaire.

SECTION 1: Respond to the questions below by ticking in the boxes provided

Please tick one

1. What is your gender

   Male ☐ Female ☐

2. Select your age by ticking any of the given group of ranges

   ☐ 18-29 ☐ 49

   ☐ 49-60 ☐ Above 60

3. What is your role in the bank?

   ☐ Senior Manager ☐ Assistant Manager/Supervisor

   ☐ Auditor/Risk Manager ☐ Operations Assistant/Clerks

4. How long have you worked for the bank?

   0-5 years ☐ 5-10 years ☐

   10 years and above ☐

SECTION 2: Your perception on fraud in CBA

5 Rat the following factors on their contribution to Fraud in the banking industry?

		High	Average	Low	No effect
6	Weak internal control and accounting systems				
7	Inadequate supervision of subordinates				
8	Disregard of customer knowledge rules				
9	Poor IT structures				
10	Poor personnel policies				
11	Low remuneration of employees				

13. Rank the reasons given in question 5 above causes of fraud in CBA in order of importance with 1 being the most important and 4 the least important

Pressure to commit fraud ----------

Rationalization of the act of fraud ----------

Opportunity to commit the fraud ----------

Others (specify) ----------

14. What is the importance given to fraud when it occurs in CBA?

Highly important ☐ moderately important ☐

Not important ☐

15. Who has the ultimately responsible/accountable fraud incidence within CBA?

Fraud Analyst ☐ Auditors ☐

Risk Analyst ☐

16. Indicate by putting a tick in the appropriate box, the extent to which you agree or disagree with the following statements about what you perceive to be the fraud management culture in CBA

	Fraud management culture	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

17	CBA has been successful in fighting fraud					
18	Fraud Investigations are completed in good time					
19	Fraud prevention is engrained in CBA's organizational culture					
20	CBA gives importance to fraud incidences in the bank					
21	Fraud policy is well communicated in CBA					
22	CBA is up to date with emerging fraud trends in the banking industry					

SECTION 3 (a): Types of fraud that affected CBA

23. Rate the prevalence of the following types of fraud in the bank?

		High	**Average**	**Low**	**No effect**
24	Management Fraud				
25	Employees fraud (insider)				
26	Employees and outsiders				
27	Employees and customers				
28.	Employees and Management				

29. Identify the prevalence of the following types of fraud committed

		High	**Average**	**Low**	**No effect**
Management Fraud					

30.	Overstatement of assets				
31	Overstatement of revenues				
32	Understatement of liabilities				
33.	Understatement of expenses				
Employee Fraud					
34.	Cash theft				
35	Forgery of customers signature				
36	Use of forged cheques to withdrawal monies				
37	Opening and operating fictitious accounts				
38.	Lending to unqualified and fictitious customers				
39.	Claiming of unearned bonuses and allowances				
40	Diversion of funds e.g. to suspence accounts				
41	Computer Frauds				
42	Misappropriate of banks assets				
Third Party Fraud					
43	Cheque fraud				
44	Kitting (using cheque clearance times to obtain loans)				
45	Misrepresentation and impersonation				
46	Use of forged documents and counterfeits				
47	Computer/money transfer frauds				

48	Clearing fraud (transferring funds to wrong beneficiaries)				
49	Letters of credit fraud				
50	Card Fraud				

SECTION 3: Prevention and Control of Fraud

Rate the effectiveness of the following fraud control measures in the Bank.

		Most Effective	**Effective**	**Least Effective**	**Not Effective**
51	Strengthening of the internal control and accounting systems				
52	Assessment and prosecution of fraud cases				
53	Tracking of fraud cases				
54	Promoting an ethical working culture in employees				
55	Encouragement of employees through communication, rewards and recognition				
56	Higher remuneration for employees				
57	Having policies to track employees conduct and background				
58	Use of performance management systems, appraisals and career development incentives				

59	Adopting well laid out hiring policies that seek the background of employees				
60	Undertaking expected and unexpected audits				
61	Implementation of employee fraud schemes i.e. schemes that track fraudulent employees across companies				
62	Establishment of a fraud policy				
63	Establishing fraud reporting centers and hotlines				
64	Ensuring shuffling and mandatory vacations for employees				
65	Use of ICT protection tools such as passwords and firewalls				
67	Use of analytical tools to detect and prevent fraud				

68. List other factors that could aid in preventing and controlling fraud in the bank?

……

……

……

……

THANK YOU FOR YOUR PARTICIPATION